Henry P. Wolfe, Esq. (NJ Atty 031942005)
Javier L. Merino, Esq. (NJ Atty 078112014)
Andrew R. Wolf, Esq. (NJ Atty 018621995)
THE DANN LAW FIRM PC
825 Georges Rd., 2nd Fl.
North Brunswick, NJ 08902
(201) 201-500-4060
notices@dannlaw.com
Attorneys for the Plaintiff

Karen Carew,

Plaintiff,

v.

Athena Bitcoin, Inc., Matias Goldenhörn, K&K Family LLC d/b/a Country Farm Convenience Store, Sukhwinder Singh d/b/a Country Farm Food N Smoke Shop, and John Doe Nos. 1 – 10.

Defendants.

UNITED STATES DISTRICT
DISTRICT OF NEW JERSEY

CIVIL ACTION

Case No.: 3:25-cv-00608-GC-JTQ

REMOVED FROM:

SUPERIOR COURT OF NEW JERSEY
LAW DIVISION, MONMOUTH COUNTY

Case No.: MON-L-003971-24

AMENDED COMPLAINT
with JURY DEMAND

The Plaintiff, Karen Carew, states for her Complaint as follows:

PARTIES and NATURE OF ACTION

1. The Plaintiff, Karen Carew, is a 75 year-old retiree from Belmar, New Jersey, who on September 4, 2024 fell victim to elaborate scam in which she was directed to deposit $39,300 of her retirement savings into Athena "Bitcoin ATM" kiosks in Asbury Park and Point Pleasant by an individual impersonating a Microsoft technical support telephone agent who convinced her that she needed to make the deposits to avoid substantial tax liability for several large deposits the agent claimed to have erroneously transferred to the Plaintiff's bank account while attempting to issue a small courtesy refund.

2. The use of Bitcoin ATMs to facilitate such crimes, known as "impersonation scams" has "skyrocketed" in recent years, according to a recent the Federal Trade Commission (FTC) report, "increasing nearly tenfold from 2020 to 2023," with reported cases "overwhelmingly about government impersonation, business impersonation, and tech support scams," and with "more than two of every three dollars reported lost to fraud using these machines… lost by an older adult." See **Exhibit A**, September 3, 2024, "FTC Data Spotlight. Bitcoin ATMs: a payment portal for scammers."
3. Defendant, Athena Bitcoin, Inc. ("Athena") is a Delaware corporation with its principal place of business in Illinois. It is among the largest operators of "Bitcoin ATM" cryptocurrency kiosks in the United States, with over 50 Bitcoin ATMs in New Jersey.
4. Athena itself has acknowledged on its website that its Bitcoin ATMs have been foreseeably and regularly been used for impersonation scams, yet has failed to implement policies and operational safeguards to prevent its Bitcoin ATMs from continuing serve as instrumentalities for these crimes, instead limiting its "efforts" to providing warnings about the scams on Bitcoin ATM screens and elsewhere, which Athena knows to have been ineffective at preventing the explosion of use of its Bitcoin ATMs to steal money from seniors and other vulnerable victims.
5. Athena has not only failed to make any real effort to detect and stop impersonation scams using its Bitcoin ATMs, but when the crimes have predictably and repeatedly occurred, Athena has retained possession of the stolen cash harvested from its machines rather than returning it to the victims, based on the misrepresentation that the cash had been "irreversibly" exchanged for Bitcoin and transferred the scammers' untraceable wallet.

6. Athena's misrepresentations that scam victims' cash was "irreversibly" transferred is particularly egregious with respect to the portion of cash *retained* by Athena as a fee (and thus not *transferred*, irreversibly or otherwise), which in the Plaintiff's case was about 25.6%
7. In the Plaintiff's case, Arthena's share of the loot from the theft was $10,060.04 of the $39,300 that Plaintiff was deceived into depositing into Athena's Bitcoin ATMs, reflecting a "fee" for providing the service to the criminals of approximately 25.6%.
8. Defendant Matias Goldenhörn is the CEO of Athena Bitcoin, Inc. and was personally involved in devising, instituting, directing, and maintaining the corporation's policies and practices alleged herein.
9. John Doe Nos. 1 through 10 are fictitious names for other individuals who were personally involved in devising, instituting, directing, and maintaining the corporation's policies and practices alleged herein, including, without limitation, some or all of Athena Bitcoin, Inc.'s past and present officers and directors. Plaintiff anticipates that these individuals will be identified through discovery, at which time she will seek leave to amend to join them by their actual names.
10. Defendant K&K Family LLC is a New Jersey limited liability company that owns and operates a convenience store business called Country Farm Convenience Store, located at 1116 Main Street, Asbury Park, New Jersey, and that has partnered with Athena by permitting it to install, operate, and maintain an Athena Bitcoin ATM kiosk inside the store, which was subsequently used to facilitate the impersonation scam perpetrated agiainst the Plaintiff
11. Defendant Sukhwinder Singh is a citizen of New Jersey, residing at 619 Butler Avenue, Point Pleasant, New Jersey, who owns and operates a convenience and vape shop business called Country Farm Food N Smoke shop, located at 3122 Route 88, Point Pleasant, New Jersey, and

who has partnered with Athena by permitting it to install, operate, and maintain an Athena Bitcoin ATM kiosk inside the store, which was subsequently used as an instrumentality in at least one impersonation scam.

12. Plaintiff brings this action for recovery of her stolen funds, enhanced damages, and other relief under various New Jersey statutory and common law causes of action.

ALLEGATIONS

13. Bitcoin ATMs are publicly accessible kiosks for converting cash to Bitcoin cryptocurrency, which is credited to an untraceable online account called a "wallet." The kiosks resemble ordinary ATMs and typically feature a touchscreen for display and input of information, a bill acceptor slot, and a scanning device for the user to input a QR code associated the "wallet."

14. The number of Bitcoin ATMs available for public use has increased dramatically in recent years, with the machines typically located at gas stations, convenience stores, vape shops, and similar establishments.

15. Bitcoin ATM operators, including Athena, have designed and marketed transactions at their kiosks to be immediate, untraceable, and irreversible (presumably to attract the type of clientele that might have use for such clandestine features) and charge much higher fees than traditional online Bitcoin exchange services (as noted earlier, Athena retained more than 25% of the cash deposited into its machines by the Plaintiff).

16. Because of their ubiquity and obvious suitability for illicit cash transfers, Bitcoin ATMs have become the instrumentality of choice for perpetrators of "impersonation scams," in which organized, sophisticated criminals pose as government, law enforcement, corporate technical support personnel and similar authority figures, and convince their victims (in most cases, seniors with retirement assets, like the Plaintiff) to withdraw large amounts of cash from their

bank accounts and deposit it into specified Bitcoin ATMs using a provided QR code, typically to prevent some legal or financial calamity concocted by the scammer.

17. The alarming explosion in the use of Bitcoin ATMs to facilitate such scams against seniors and other vulnerable groups has been the subject of numerous, well-publicized reports by federal and state financial and law enforcement agencies over the past several years, most recently by the Federal Trade Commission (FTC), which in September of 2024 issued a data report stating that FTC "data show that fraud losses at BTMs are skyrocketing, increasing nearly tenfold from 2020 to 2023," that "[r]eports of losses using BTMs are overwhelmingly about government impersonation, business impersonation, and tech support scams," and that "people 60 and over were more than three times as likely as younger adults to report a loss using a BTM. In fact, more than two of every three dollars reported lost to fraud using these machines was lost by an older adult." See **Exhibit A**, Federal Trade Commission, September 3, 2024, "FTC Data Spotlight. Bitcoin ATMs: a payment portal for scammers."[1]

18. Athena itself has openly acknowledged since at least 2018 that its Bitcoin ATM kiosks not only pose a high risk of use as instrumentalities for impersonation scams, but in fact have been regularly used for such crimes.

19. For example, a page on Athena's website entitled "Avoid these Bitcoin Scams" states,

---

[1] See also, e.g., **Exhibit B,** Federal Bureau of Investigation (FBI), I-100421-PSA, November 4, 2021 "The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment" (warning, "The FBI has seen an increase in scammers directing victims to use physical cryptocurrency ATMs and digital QR codes to complete payment transactions."); **Exhibit C**, New Jersey Commission of Investigation, February 2021, "Bitcoin ATMs: Scams, Suspicious Transactions, and Questionable Practices at Cryptocurrency Kiosks" ("The Commission examined hundreds of records subpoenaed from… cryptocurrency kiosk [operators] in New Jersey over the last five years" and found "numerous instances where unwitting victims were duped into sending cryptocurrency to unknown wallets through the machines, including some schemes that resulted in the loss of tens of thousands of dollars.")

> Scammers are looking to say and do anything to convince you of an urgent need to pay through Bitcoin, and they will often "helpfully" point out nearby ATMs where you can follow their commands.
>
> Scam artists like Bitcoin because transactions cannot be cancelled, reversed, or otherwise refunded once made.
>
> ***Athena receives numerous reports of fraud per month***, so we want to share much of what we've learned to look out for…[2]

(emphasis added). The page then describes common types of Bitcoin ATM scams, one of which, the "Tech Support / Bank Impersonation Scam" is highlighted with a red box containing blue text that reads, "This has been the most common scam of 2022!" and describes the same technics employed against the Plaintiff *two years later* that resulted in the theft from her of $39,300 facilitated by Athena Bitcoin ATMs. See **Exhibit D**, www.athenabitcoin.com/avoid-these-bitcoin-scams (as it appeared from at least 2022 through the date of filing of this pleading).

20. A former version of the "Avoid these Bitcoin Scams" page that appeared on Athena's website from 2018 through at least August 8, 2021 stated that "Athena is the gateway for tens of thousands of customers to the world of Bitcoin" and therefore "some customers end up unwittingly victims of fraud perpetuated by con artists" who "like Bitcoin because transactions cannot be cancelled, reversed, or otherwise refunded once broadcast." The page then described several common "Impersonation scams." See **Exhibit E,** athenabitcoin.com/news/2018/3/29

---

[2] Athena has admitted in filing in this action that "at least 100 individuals have self-reported" to Athena that their money was stolen in a scam facilitated by "Athena Bitcoin's kiosks in New Jersey during" since January 2019 (without conceding that these individuals "were in fact defrauded"). ECF Doc. 13 (Pre-motion Response Letter), page 2. During that same period, Athena reports that 1,300 individuals "used" Athena's New Jersey kiosks. *Id.* Thus, Athena had reason to believe that 1 of every 13 (or 7.64%) users of its New Jersey kiosks were unwitting victims of the impersonation scams.

/avoid-these-bitcoin-scams, as it appeared on August 8, 2021 (retrieved from web.archive.org).

21. On another page of the website entitled "Fraud Alert," Athena acknowledges, "Imposter scams are the most common Bitcoin fraud that we see!" and describes the scams in chilling terms, from the victims' point of view:

> Imagine being in a panic thinking that you will be arrested or that money is about to be drained out of your bank account? Imagine having someone on the phone with you for hours making sure you obey their instructions? Thousands of people each year don't have to imagine…."

Exhibit F, www.athenabitcoin.com/the-most-common-bitcoin-scam-that-we-see, as it appeared from at least 2022 through the date of filing of this pleading.

22. In contrast to the high degree of danger they pose by facilitating and thus promoting crime against seniors and others vulnerable individuals, Athena's Bitcoin ATMs have little or no apparent utility.

23. Athena's website describes the supposed utility of its Bitcoin ATMs using vague generalities, claiming that they provide "unprecedented financial independence," "unmatched convenience," "fast and seamless transactions" and "financial inclusion," without providing examples of any specific tasks, goals, or purposes that Athena's customers typically accomplish by exchanging cash for Bitcoin on a machine in a vape shop, for an exorbitant fee. See www.athenabitcoin.com/unlock-financial-freedom-with-athena-bitcoin-atms/ (last visited November 20, 2024).[3]

24. Athena's admissions that its Bitcoin ATMs are regularly used as instrumentalities for "impersonation scams" have been corroborated by news reports of such incidents, as well as other court actions against Athena. See e.g., www.coalregioncanary.com/2024/07/25/athena-

[3] Ironically, impersonation and other scams appear to be the only examples on Athena's website of *specific* purposes for which its Bitcoin ATMs have been used.

bitcoin-scam-schuylkill-county-minersville-atm-machine/; (last visited November 20, 2024); www.local10.com/news/local/2024/08/02/police-georgia-woman-impersonated-deputies-to-target-fraud-victims-with-fake-warrants/ (last visited November 20, 2024; *Hoist v. Athena Bitcoin ATM*, 23-cv-21905-RK-RLS (D.N.J. 2023).

25. Despite knowing for over six years that its Bitcoin ATM kiosks have regularly and foreseeably been used by criminals as instrumentalities in impersonation scams, Athena has failed to remediate the extreme danger that its Bitcoin ATMs have posed to seniors and other vulnerable populations.

26. Despite its express knowledge of the regular and foreseeable use of its Bitcoin ATM kiosks as instrumentalities in impersonation scams, Athena has failed to implement design, operational, or policy changes that would preclude such use, for example, by detecting and rejecting suspicious transactions (such as the four transactions directed by the Plaintiff's scammer, in which a total of $39,300 was deposited in 6.5 hours span on the same day by a first-time 74 year old user), implementing strict and accurate identification requirements and mechanisms, placing strict limits on the amounts of deposits by new users for an introductory period, placing strict limits on total daily deposits for all users, implementing policies and mechanisms to confirm that the wallet belongs to the depositor, and implementing a reasonable holding period before the cash is converted to bitcoin and "irreversibly" transferred.

27. Instead of taking effective, responsible measures to eliminate the danger posed by its Bitcoin ATMs, Athena has limited its "efforts" to passive measures that have been ineffective at stopping the regular and foreseeable use of its kiosks to enable scams.

28. Athena's efforts to address the regular and foreseeable use of its Bitcoin ATMs to enable scams have been limited to displaying warnings about such scams at the beginning of each

transactions and requiring users to click several check boxes next to disclaimers stating that the user has been warned about scams, that the wallet to be used in the transaction belongs to the user, and similar affirmations.

29. Such warnings, disclaimers, and checkboxes are predictably ineffective in the context of an impersonation scam, in which the victim is not engaging with the kiosk as a voluntary customer, but rather at the explicit direction of a professional criminal who the victim believes must be obeyed to avert financial disaster, as Athena itself has empathetically acknowledges on its website:

> Imagine being in a panic thinking that you will be arrested or that money is about to be drained out of your bank account? Imagine having someone on the phone with you for hours making sure you obey their instructions? Thousands of people each year don't have to imagine…."

See **Exhibit F,** athenabitcoin.com/the-most-common-bitcoin-scam-that-we-see.

30. Athena's warnings and disclaimers have in fact been largely ineffective in eliminating the extreme danger posed by its Bitcoin ATMs to seniors and others vulnerable to impersonation scams facilitated by Athena's machines.

31. Notably, the explosion of scams recently reported by the FTC largely occurred *after* Althea implemented its impotent and ineffective warnings, disclaimers, and checkboxes.

32. Athena is capable of implementing effective and sufficient checks and procedures that would intervene, prevent, mitigate, or deter the use of its Bitcoin ATMs in impersonation, but has chosen not to adopt such measures because doing so would thwart a substantial volume of Athena's business and the considerable profit it gains from every dollar inserted into the machines.

33. On September 11, 2024, in the wake of the recent FTC report, members of the United States Senate Banking Committee sent a letter to Athena (attached as **Exhibit G)** calling on the

company **"**to take immediate action to address troubling reports that your Bitcoin ATMs (BTMs) are contributing to widespread financial fraud against elderly Americans" and asking for information regarding "what actions Athena Bitcoin is taking to address this problem" by October 4, 2024. In addition asking for information regarding warnings that Athena provides regarding use of its kiosks for scams, the letter asked whether "Athena Bitcoin limit[s] the amount an individual can deposit or transfer in a single day, week, or other period of time," whether "Athena Bitcoin hold[s] deposited and transferred funds for any period of time or take[s] any other measures to allow transactions to be reversed in the case of fraud or mistake" and whether "Athena Bitcoin insure depositors against fraud[.]"

34. To Plaintiff's knowledge, Athena has not responded to the Senators' inquiry.

Allegations Relating to the Theft of the Plaintiff's Money

35. On the morning of September 4, 2024, the Plaintiff, Karen Carew attempted to use her personal computer at her home in Belmar, New Jersey, and found that she was unable to access Microsoft Windows. A message appeared on the display advising her that a technical problem had been detected and directing her to contact technical support at a telephone number specified in the message.

36. Plaintiff called the number and spoke with a man who identified himself as a Microsoft technical service representative.

37. After the Plaintiff described the issue with her computer, the purported Microsoft representative assured her that he would assist in resolving the problem, and that Microsoft would be issuing her a refund for the inconvenience and temporary loss of use of her computer and software.

38. The purported Microsoft representative requested the Plaintiff's bank account information to process the refund, which she provided.

39. Shortly after the Plaintiff provided her banking information, the purported Microsoft representative, in a distraught tone of voice, told her that he erroneously processed the refund for $10,200 instead of $102. At the suggestion of the purported Microsoft representative, the Plaintiff logged into her bank account and confirmed that $10,200 had just been electronically transferred to the account.

40. The purported Microsoft representative then told the Plaintiff that because of the amount of the overpayment, it would be reported to the I.R.S. and she would be subject to substantial tax liability if she did not pay back the overpayment immediately.

41. The purported Microsoft representative then advised her that in order for the repayment to be processed in time to avoid I.R.S. detection and tax liability, it would have to be made in cash, by depositing it into an Athena ATM for transfer to an associated Microsoft business account.

42. For the next seven hours, the purported Microsoft representative remained on the phone with the Plaintiff (with a few periods where they were disconnected) and directed her to drive to different branches of her bank, withdraw various quantities of cash, and deposit the cash into two different Athena Bitcoin ATMs using a QR code that she received via text message.

43. The initial deposit was for $10,100 in cash, which the Plaintiff inserted in one transaction into a Athena Bitcoin ATM kiosk located on the premises of Defendant Country Farm Convenience Store convenience at 1116 Main Street, Asbury Park, New Jersey, which was completed on January 4, 2024 at approximately 12:04 p.m.

44. After making the initial "repayment" of $10,100, the purported Microsoft representative convinced the Plaintiff to continue to withdraw cash from her bank account and deposit it into

Athena Bitcoin ATMs using the provided QR code, by convincing her of additional overpayments to her bank account, each of which appeared to be confirmed based on her review of her account online, and by the availability of the funds for the several cash withdrawals she made that day.

45. By the end of the day on September 4, 2024, the Plaintiff had withdrawn a total of $39,300 from her bank account and deposited the same amount into Athena Bitcoin ATMs in four separate deposits, including three at the kiosk in Country Farm Convenience Store convenience at 1116 Main Street, Asbury Park, New Jersey Asbury Park and one at Country Farm Food N Smoke Shop, at 3122 NJ Hwy 88, Point Pleasant, New Jersey.
46. These included the initial deposit of $10,100 at 12:04 p.m. in Asbury Park, a deposit of $9,000 at 1:39 p.m. in Asbury Park, a deposit of $11,200 at 3:58 p.m. in Point Pleasant, and a deposit of $9,000 at 6:29 p.m. in Asbury Park.
47. Plaintiff made these large, protracted deposits of cash into the machines in the presence of the Country Farm stores' managers.
48. Although each of the transactions required insertion of numerous paper bills and took considerable time, the Defendants' staff did nothing to intervene or inquire about the suspicious deposits.
49. Later in the evening on September 4, 2024, the Plaintiff became aware that she had been the victim of a scam while speaking about what had transpired with her son.
50. Plaintiff then reported the incident to the Belmar Police Department on September 5, 2024, who advised her that it would make a report and investigate the incident.
51. The Belmar Police Department subsequently caused a subpoena to be served on Athena seeking information pertaining to the Department's investigation.

52. The Plaintiff's adult daughter subsequently reported the incident to the FBI, on the Plaintiff's behalf

53. To date, neither the FBI nor the Belmar Police Department have identified the imposter or the ultimate recipient of the Bitcoin transferred by Athena during the scam.

Allegations Relating to Athena's Possession of the Plaintiff's Stolen Property

54. After the theft of Plaintiff's $39,300 in cash on September 4, 2024, Athena retained possession of the stolen cash and converted it to its own use, rather than turning it over to the police or Plaintiff.

55. Athena has retained and failed to turn over the stolen cash to the police or Plaintiff despite having been notified of the theft.

56. Athena has retained and failed to turn over the stolen cash to the police or Plaintiff despite having been notified that the Plaintiff deposited the cash into Athena's Bitcoin ATMs under a mistake as to the identity of the recipient.

57. Athena has maintained a policy and practice of retaining cash inserted into its Bitcoin ATMs as a result of impersonation scams rather than returning it to the victims, based on Athena's position, stated in the written warnings given at its Bitcoin ATMs, that all cash deposited into the machines is "irreversibly" transferred as Bitcoin to the designated wallet.

58. Athena's statements that cash deposits at its Bitcoin ATMs are irreversible is misleading, as the cash itself remains physically inside the kiosk, and thus in Athena's possession and control.

59. Athena's misrepresentations are particularly apparent with respect to the substantial portion of the stolen cash that was retained by Athena as a fee for its "services" and thus not transferred to the scammer, irreversibly or otherwise.

60. In the Plaintiff's case, Arthena's share of the loot from the theft was $10,060.04 (about 25.6%) of the $39,300 stolen from the Plaintiff's retirement funds her retirement funds.

61. According to the permanent ledger of cryptocurrency transactions accessible online, called "blockchain," Athena converted and transferred as Bitcoin to the scammer's wallet only a portion of each of the four cash deposits made by Plaintiff on September 4, 2024.

62. Of the $10,100 deposited by Plaintiff on September 4, 2024 at 12:04 p.m., Athena transferred only $7,473.28 in Bitcoin to the scammer's wallet address.

63. Of the $9,000 deposited by Plaintiff on September 4, 2024 at 1:39 p.m., Athena transferred only $6,695.96 in Bitcoin to the scammer's wallet address.

64. Of the $11,200 deposited by the Plaintiff on September 4, 2024 at 3:58 p.m., Athena transferred only $8,365.49 in Bitcoin to the scammer's wallet address.

65. Of the $9,000 deposited by Plaintiff on September 4, 2024 at 6:29 p.m., Athena transferred only $6,705.23 in Bitcoin to the scammer's wallet address.

66. Athena therefore did not transfer to the scammer, irreversibly or otherwise, at least $10,060.04 of the value of the $39,300 in cash deposited into Athena's Bitcoin ATMs during the course of the scam perpetrated against the Plaintiff on September 4, 2024.

CAUSES OF ACTION

FIRST COUNT: Civil Action for Possession of Stolen Property (N.J.S.A. 2C:20-20)

67. N.J.S.A. 2C:20-20 creates a civil right of action for triple damages, reasonable attorney's fees, and costs for "[a]ny person damaged in his business or property by reason of a violation of section 7 of this…act, " which refers N.J.S.A. 2C:20-7 and N.J.S.A. 2C:20-7.1, criminal

statutory provisions prohibiting various theft related activities, including receiving stolen property (N.J.S.A. 2C:20-7) and "trafficking" in stolen property (N.J.S.A. 2C:20-7.1(b)).

68. "Trafficking" as used in N.J.S.A. 2C:20-7-1(b) is broadly defined, and includes the following conduct: "1. [t]o sell, transfer, distribute, dispense or otherwise dispose of property to another person, or 2. to buy, receive, possess, or obtain control of or use property, with intent to sell, transfer, distribute, dispense or otherwise dispose of such property to another person." N.J.S.A. 2C:20-1.

69. In a civil action under N.J.S.A. 2C:20-20, "*[a]ll persons who have possessed or obtained control of stolen property are liable as principals* and may be sued jointly or severally, whether or not possession or control was joint," subject to a right to sue the principal for contribution. N.J.S.A 2C:20-20(b)(1)(emphasis added).

70. The unidentified scammer who deceived Plaintiff into depositing her cash into Athena's Bitcoin ATMs violated N.J.S.A. 2C:20-7 and N.J.S.A. 2C:20-7.1 by, without limitation, receiving stolen property and trafficking in stolen property.

71. Athena violated N.J.S.A. 2C:20-7 and N.J.S.A. 2C:20-7.1 by, without limitation, receiving stolen property and trafficking in stolen property.

72. The Plaintiff was damages by reasons of these violations of N.J.S.A. 2C:20-7 and N.J.S.A. 2C:20-7.1 committed by the unidentified scammer, Athena, or both,

73. The Plaintiff suffered damages in the amount of the $39,300 that was stolen from her by the scammer using Athena's Bitcoin ATMs.

74. In the alternative, Plaintiff suffered damages in the amount of $10,060.04, which is the portion of the stolen money that Athena retained as its "fee" and continued to retain after Athena learned the money was stolen.

75. The Plaintiff is therefore entitled to a judgment against Athena for triple the money that was stolen from them, reasonable attorney's fees, and costs, pursuant to N.J.S.A. 2C:20-20.

SECOND COUNT: New Jersey Racketeer Influenced and Corrupt Organizations Act

76. The New Jersey Racketeer Influenced and Corrupt Organizations Act ("NJRICO") provides, at N.J.S.A. 2C:41-2(c) that "[i]t shall be unlawful for any person employed by or associated with any enterprise engaged in or activities of which affect trade or commerce to conduct or participate, directly or indirectly, in the conduct of the enterprise's affairs through a pattern of racketeering activity..."

77. Defendant Athena Bitcoin, Inc. Defendant Matias Goldenhörn, and Defendants John Doe Nos. 1 - 10 are each "persons" as defined by NJRICO, N.J.S.A. 2C:41-1(b).

78. Defendant Athena Bitcoin, Inc. Defendant Matias Goldenhörn, and Defendants John Doe Nos. 1 - 10 are collectively an "enterprise" as defined by NJRICO, at N.J.S.A. 2C:41-1(c), with respect to their policies and practices relating to trafficking in, possessing, and retaining stolen property, and their failure to mitigate the foreseeable risk of harm to the public created by their "services," their, as alleged herein.

79. Defendant Athena Bitcoin, Inc. is, independently, an "enterprise" as defined by NJRICO, at N.J.S.A. 2C:41-1(c), with respect to its policies and practices relating to its trafficking in, possessing, and retaining stolen property, and its failure to mitigate the foreseeable risk of harm to the public created by its "services," as alleged herein.

80. NJRICO defines "racketeering activity" to include, inter alia, "theft and all crimes defined in chapter 20 of Title 2C of the New Jersey Statutes" as well as "fraudulent practices and all crimes defined in chapter 21 of Title 2C of the New Jersey Statutes."

81. By engaging in the conduct alleged herein, the Defendants have engaged in "racketeering activity," including, without limitation, the following:

    a. Theft of property lost, mislaid, or delivered by mistake, N.J.S.A. 2C:20-6 ("A person who comes into control of property of another that he knows to have been…delivered under a mistake as to the nature or amount of the property or the identity of the recipient is guilty of theft if, knowing the identity of the owner and with purpose to deprive said owner thereof, he converts the property to his own use.");

    b. Receiving stolen property, N.J.S.A. 2C:20-7;

    c. Trafficking in stolen property, N.J.S.A. 2C:20-7.1;

    d. Deceptive business practices, N.J.S.A. 2C:21-7(h)("A person commits an offense if in the course of business he… makes a false or misleading written statement for the purpose of obtaining property or credit" such as the Defendants numerous written statement falsely and misleadingly stating that all cash deposited into Athena Bitcoin ATMs by scam victims are "irreversible")

82. Defendant Athena Bitcoin, Inc. Defendant Matias Goldenhörn, and Defendants John Doe Nos. 1 - 10 engaged in activities, directly or indirectly, in the conduct of the enterprise's affairs through a pattern of racketeering activity, including violations of N.J.S.A. 2C:20-6, 20-7, 20-7.1, and/or 21-7(h) on at least two occasions within the 10 years of filing of this action, and therefore engaged "directly or indirectly" in "a pattern of racketeering activity" as defined by NJRICO, at N.J.S.A. 2C:41-1(d).

83. In addition to the Defendants' racketeering activities in connection with the money stolen from the Plaintiff, as alleged herein, the Defendants engaged, directly or indirectly, in the same or substantially similar activities in connection with one or more other victim of scams using

Athena Bitcoin ATMs in New Jersey. See e.g., *Hoist v. Athena Bitcoin ATM*, :23-cv-21905-RK-RLS (D.N.J. 2023).

84. The Plaintiff suffered damages from Defendants' violations of NJRICO in the amount of the $39,300 that was stolen from her with the aid of Athena's Bitcoin ATMs.

85. In the alternative, Plaintiff suffered damages in the amount of $10,060.04, which is the portion of the stolen money that Athena retained as its "fee" and continued to retain after Athena learned the money was stolen.

86. The Plaintiff is therefore entitled to all appropriate legal and equitable relief, an award of treble their damages, plus attorney's fees, and costs pursuant to N.J.S.A. 2C:41-4(c).

THIRD COUNT: Negligence / Gross Negligence / Recklessness

87. At all times relevant to this action, Defendant Athena and Defendant Goldenhörn and Defendants John Doe Nos. 1 - 10 were expressly aware of the regular and foreseeable use of Athena Bitcoin ATMs as instrumentalities in impersonation scams.

88. Defendants had a duty to Plaintiff to take reasonable design, policy, and procedural steps to prevent Athena Bitcoin ATMs from continuing to be regularly used by criminals as instrumentalities in impersonation scams.

89. Defendants had a duty to reasonably and effectively mitigate the high risk of harm to the public admittedly caused by their Bitcoin ATM's attractiveness to scammers.

90. Defendants breached their duty to the Plaintiff by negligently, recklessly, and knowingly failing to implement checks and procedures both at its ATMs and internally that would effectively intervene, mitigate, or deter the use of its ATMs in highly foreseeable scams, such as the one that Plaintiff fell victim to.

91. At all times relevant to this action, Defendants K&K Family LLC d/b/a Country Farm Convenience Store and Sukhwinder Singh d/b/a Country Farm Food N Smoke Shop (collectively, the "Convenience Store Defendants") knew or should have known of the regular and foreseeable use of Athena's Bitcoin ATM's as instrumentalities in impersonation scams against elderly and other vulnerable individuals.
92. Each Convenience Store Defendant owns and maintains control over the convenience store at which the Athena ATMs are located.
93. The Plaintiff is deemed to have been an invitee when she entered the convenience stores, and the Convenience Store Defendants therefore owed her a high duty of care, requiring the store Defendants to maintain the premises in a safe condition and take active steps to ensure her safety while on the property.
94. The transactions at issue in this case, in which a senior citizen with no prior or subsequent transaction history inserted $39,300 in cash, bill-by-bill, into two Athena Bitcoin ATMs in a single afternoon, were atypical and suggestive of a scam and the Convenience Store Defendants had a duty to inquire, intervene, and/or deter the transactions.
95. The thefts would have been detected and deterred if the Convenience Store Defendants' had not breached their duty of care owed to the Plaintiff.
96. The Plaintiff was damaged by all Defendants' breaches described above, in the amount of the cash that was stolen from them using Athena Bitcoin ATMs.
97. Defendants' negligent, reckless, and knowing failure and refusal to implement appropriate and sufficient checks and procedures to intervene, mitigate, or deter the use of the ATMs described above in the subject scams was a direct and proximate cause of Plaintiff damages.

FOURTH COUNT: New Jersey Consumer Fraud Act

98. The Consumer Fraud Act (CFA), at N.J.S.A. 56:8-2, broadly prohibits "any commercial practice that is unconscionable or abusive, deception, fraud, false pretense, false promise [or] misrepresentation… in connection with the sale or advertisement of any merchandise… or with the subsequent performance."

99. The CFA defines "sale..of any merchandise" broadly, and the term includes the Defendants' sale of cryptocurrency exchanges and transfers through Athena's Bitcoin ATM machines.

100. N.J.S.A. 56:8-19 provides for a private right of action for treble damages, equitable relief, and reasonable attorney's fees and costs to "[a]ny person who suffers any ascertainable loss of moneys or property, real or personal, as a result of the use or employment by another person of any method, act, or practice declared unlawful under this act."

101. The plain language of the CFA does not require privity between "any person" who violates the Act and the "any person" who suffers "ascertainable loss…as a result of" the violation.

102. Defendants engaged in unconscionable commercial practices, abusive commercial practices, and/or deception in violation of the CFA at N.J.S.A. 56:8-2, including, without limitation:

a. Failure and refusal to implement appropriate and sufficient checks and procedures to intervene, mitigate, and/or deter the use of the Athena Bitcoin ATMs in the subject scams;

b. Failure to intervene, and/or deter the transactions occurring in the Convenience Store Defendants' establishments when it was apparent that they were suspicious and indicative of scams;

c. Offering a service that is known, in fact designed, to facilitate illicit cash transfers, and then refusing to take reasonable measures to mitigate the foreseeable risk of harm to the public caused by the criminals the service admittedly attracts;

d. Refusing to return the "fee" of 25% of the money that was stolen from Plaintiff, after learning it was stolen.

103. Under CFA precedents, violation of other laws can establish or serve as evidence of abusive and/or unconscionable commercial practices.

104. Defendants further engaged in abusive and/or unconscionable commercial practices by engaging in the following conduct prohibited under New Jersey law:

a. Theft of property lost, mislaid, or delivered by mistake, N.J.S.A. 2C:20-6 ("A person who comes into control of property of another that he knows to have been…delivered under a mistake as to the nature or amount of the property or the identity of the recipient is guilty of theft if, knowing the identity of the owner and with purpose to deprive said owner thereof, he converts the property to his own use.");

b. Receiving stolen property, N.J.S.A. 2C:20-7;

c. Trafficking in stolen property, N.J.S.A. 2C:20-7.1;

d. Deceptive business practices, N.J.S.A. 2C:21-7(h)("A person commits an offense if in the course of business he… makes a false or misleading written statement for the purpose of obtaining property or credit" such as the Defendants numerous written statement falsely and misleadingly stating that all cash deposited into Athena Bitcoin ATMs by scam victims are "irreversible")

105. The Plaintiff suffered ascertainable loss from Defendants' violations of the CFA in the amount of the $39,300 that was stolen from her with the aid of Athena's Bitcoin ATMs, or in

the alternative, in the amount of $10,060.04, which is the portion of the stolen money that Athena retained as its "fee" and continued to retain after Athena learned the money was stolen.

106. The Plaintiff is thus entitled to all appropriate legal and equitable relief, an award of treble their damages, plus attorney's fees, and costs pursuant to N.J.S.A. 56:8-19.

PRAYER FOR RELIEF

The Plaintiff requests judgment as follows:

a. As to the First Count, judgment against Defendant Athena, Defendant Goldenhörn, and Defendants John Doe Nos. 1 – 10, jointly and severally, for treble damages under N.J.S.A. 2C:20-20 in favor of the Plaintiff;

b. As to the Second Count, judgment against Defendant Athena, Defendant Goldenhörn, and Defendants John Doe Nos. 1 – 10, jointly and severally, for treble damages under NJRICO at N.J.S.A. 2C:41-4 in favor of the Plaintiff.

c. As to the Third Count, judgement for actual damages against all Defendants, and judgment for actual and punitive damages against Defendants Athena, Defendant Goldenhörn, and Defendants John Doe Nos. 1 – 10;

d. As to the Fourth Count, judgment against all Defendants for treble damages under the CFA at N.J.S.A. 56:8-19, in favor of the Plaintiff, as well as an injunction prohibiting the Defendants from continuing to engage in the unlawful acts complained of herein within the State of New Jersey;

e. Reasonable attorney fees and costs, as mandated under N.J.S.A. 2C:20-20, N.J.S.A. 2C:41-4, N.J.S.A. 56:8-19, or otherwise authorized by law;

f. Pre-judgment and post-judgment interest; and

g. All other relief as the Court deems just and equitable.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

NOTICE TO ATTORNEY GENERAL OF ACTION

A copy of the Amended Complaint will be e-mailed to the Attorney General of the State of New Jersey within 24 hours after the filing with the Court, pursuant to N.J.S.A. 56:8-20.

Dated: March 7, 2025

s/ Henry P. Wolfe
Henry P. Wolfe, Esq.
The Dann Law Firm, P.C.

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Consumer Protection Data Spotlight
FTC reporting back to you

Data Spotlight

Bitcoin ATMs: A payment portal for scammers

By: Emma Fletcher | September 3, 2024

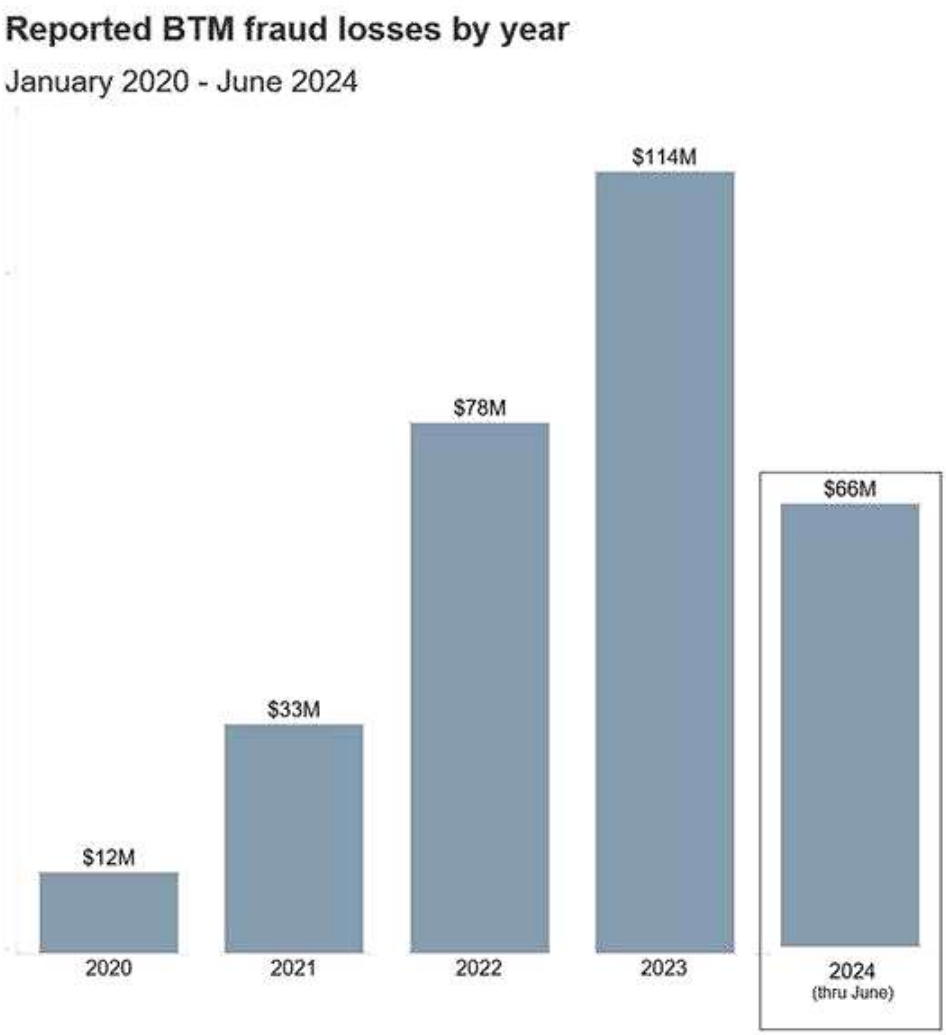
Bitcoin ATMs (or BTMs)[1] have been popping up at convenience stores, gas stations, and other high-traffic areas for years.[2] For some, they're a convenient way to buy or send crypto, but for scammers they've become an easy way to steal. FTC Consumer Sentinel Network data show that fraud losses at BTMs are skyrocketing, increasing nearly tenfold from 2020 to 2023, and topping $65 million in just the first half of 2024.[3] Since the vast majority of frauds are not reported, this likely reflects only a fraction of the actual harm.[4]

Cryptocurrency surged as a major payment method for scams in recent years, along with the massive growth in crypto payments on fake investment opportunities.[5] But now crypto is a top payment method for many other scams, too.[6] Widespread access to BTMs has helped make this possible. Reports of losses using BTMs are overwhelmingly about government impersonation, business impersonation, and tech support scams.[7] And when people used BTMs, their reported losses are exceptionally high. In the first six months of 2024, the median loss people reported was $10,000.[8]

In the first half of the year, people 60 and over were more than three times as likely as younger adults to report a loss using a BTM.[9] In fact, more than two of every three dollars reported lost to fraud using these machines was lost by an older adult.[10]

Scams that use BTMs work in lots of different ways. Many start with a call or message about supposed suspicious activity or unauthorized charges on an account.[11] Others get your attention with a fake security warning on your computer, often impersonating a company like Microsoft or Apple. These things are hard to ignore, and that's the point. From there, the story quickly escalates. They might say all your money is at risk, or your information has been linked to money laundering or

Give Feedback



even drug smuggling. The scammer may get a fake government agent on the line – maybe even claiming to be from the "FTC" – to up the ante.

So where do BTMs fit into the story? Scammers claim that depositing cash into these machines will protect your money or fix the fake problem they've concocted. They've even called BTMs "safety lockers." They direct you to go to your bank to take out cash. Next, they send you to a nearby BTM location – often a specific one – to deposit the cash you just took out of your bank account.[12] They text you a QR code to scan at the machine, and once you do, the cash you deposit goes right into the scammer's wallet.

So how can you spot and steer clear of these scams?

- Never click on links or respond directly to unexpected calls, messages, or computer pop-ups. If you think it could be legit, contact the company or agency, but look up their number or website yourself. Don't use the one the caller or message gave you.

- Slow down. Scammers want to rush you, so stop and check it out. Before you do anything else, talk with someone you trust.
- Never withdraw cash in response to an unexpected call or message. Only scammers will tell you to do that.
- Don't believe anyone who says you need to use a Bitcoin ATM, buy gift cards, or move money to protect it or fix a problem. Real businesses and government agencies will never do that – and anyone who asks is a scammer.

To spot and avoid scams visit ftc.gov/scams. Report scams to the FTC at ReportFraud.ftc.gov.

---

[1] While machines that allow consumers to buy cryptocurrency are commonly referred to as Bitcoin ATMs or BTMs, these machines often handle – and scams can take place in – other cryptocurrencies in addition to Bitcoin.

[2] BTM installations self-reported by operators to an industry website increased from about 4,250 in January 2020 to about 32,000 in June 2024. See trend chart available at https://coinatmradar.com/charts/growth/united-states/

[3] These and other figures throughout this Spotlight are estimates based on keyword analysis of the narratives provided in reports that identified cryptocurrency as the payment method. Not all reports identify a payment method or include sufficient details in the report narrative to determine whether a BTM was used.

[4] See Anderson, K. B., To Whom Do Victims of Mass-Market Consumer Fraud Complain? at 1 (May 2021), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3852323(study showed only 4.8% of people who experienced mass-market consumer fraud complained to a Better Business Bureau or a government entity).

[5] See FTC Consumer Protection Data Spotlight, Reports Show Scammers Cashing in on Crypto Craze (June 3, 2022), available at https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammerscashing-crypto-craze.

[6] In the first half of 2024, cryptocurrency was the top payment method in terms of aggregate reported losses on tech support scams and job scams, and the second most costly method after bank transfers on business impersonation scams, government impersonation scams, romance scams, and family and friend impersonation scams.

[7] In the first half of 2024, about 86% of people who reported a fraud loss using a BTM indicated that it was on a government impersonation, business impersonation, and/or tech support scam. This excludes reports categorized as unspecified.

[8] In the first half of 2024, the median individual reported fraud loss when cryptocurrency was the reported payment method (including reports with and without BTM use) was $5,400; the median individual reported loss to fraud generally was $447.

[9] This comparison of older and younger consumers' reporting rates is normalized based on the population size of each age group using the Census Bureau's 2018-2022 American Community Survey 5-Year Estimates. This excludes reports that did not include consumer age information.

[10] In the first half of 2024, people 60 and over reported losing $46 million using BTMs, or about 71% of the reported losses using these machines. During the same period, when a reported cryptocurrency fraud loss did not involve the use of a BTM, about 72% of the losses were reported by people 18 to 59. Most of these losses were to fake cryptocurrency investment opportunities. Percentage calculations exclude reports that did not include consumer age information.

[11] Phone calls were the initial contact method in about 47% of these reports, followed by online ads or pop-ups (16%), and e-mails (9%). Reports indicating online ad or pop-up as the contact method typically described fake computer security alerts. People reported that security pop-ups and email messages included a phone number to call for help.

[12] Reports show that scammers direct people to specific BTM locations and many consumers name the BTM operator in their reports. These details show a pattern that suggests scammers prefer some operators over others and that these preferences have changed over time. While the reports do not tell us why this might be, differences in fraud prevention measures taken by various operators likely play a role.

Tags: Consumer Protection | Bureau of Consumer Protection | Imposter | Money Transfers | Consumer Sentinel Network | deceptive/misleading conduct | Finance | Credit and Finance | Privacy and Security | Tech | FinTech

Bitcoin ATMs: A payment portal for scammers (317.55 KB)

More from the Data Spotlight

Data Spotlight

Who's who in scams: a spring roundup

Emma Fletcher | May 24, 2024

Data Spotlight

Impersonation scams: not what they used to be

April 1, 2024

Data Spotlight

Social media: a golden goose for scammers

Emma Fletcher | October 6, 2023

Data Spotlight

IYKYK: The top text scams of 2022

Emma Fletcher | June 8, 2023

Give Feedback

Get Business Blog updates

Enter email address

Subscribe

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

November 4, 2021

Alert Number
I-110421-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment

The FBI warns the public of fraudulent schemes leveraging cryptocurrency ATMs and Quick Response (QR) codes to facilitate payment. The FBI has seen an increase in scammers directing victims to use physical cryptocurrency ATMs and digital QR codes to complete payment transactions.

A QR code is a square barcode with information that can be scanned and read with a smartphone camera. An individual can scan the QR code of an intended recipient to auto-populate the recipient field making it easier to send cryptocurrency to the correct destination. QR codes can be used at cryptocurrency ATMs to direct payment to an intended recipient. While many businesses have legitimately used QR code payment in the last year because of the COVID-19 pandemic, QR codes also play a role in malicious use of cryptocurrency payments.

Criminal actors, in various fraudulent schemes, maliciously leverage cryptocurrency ATMs and QR codes to receive payments from victims. Such schemes include online impersonation schemes (scammer falsely identifies as a familiar entity such as the government, law enforcement, a legal office, or a utility company), romance schemes (scammer establishes an online relationship with a victim by creating a false sense of intimacy and dependency), and lottery schemes (scammer falsely convinces a victim that they have won an award and consequently demands the victim to pay lottery fees).

Regardless of the scheme, the methods using cryptocurrency ATMs and QR codes appear similar. The scammer often requests payment from the victim and may direct the victim to withdraw money from the victim's financial accounts, such as investment or retirement accounts. The scammers provide a QR code associated with the scammer's cryptocurrency wallet for the victim to use during the transaction. The scammer then directs the victim to a physical cryptocurrency ATM to insert their money, purchase cryptocurrency, and use the provided QR code to auto-populate the recipient address. Often the scammer is in constant online communication with the victim and provides step-by-step instructions until the payment is completed.

Cryptocurrency's decentralized nature creates challenges that makes it difficult to recover. Once a victim makes the payment, the recipient instantly owns the cryptocurrency, and often immediately transfers the funds into an account overseas. This differs from traditional bank transfers or wires where a payment transaction can remain pending for one to two days before settlement. It can also make law enforcement's recovery of the funds difficult and can leave many victims with a financial loss.

Tips to Protect Yourself:

- Do not send payment to someone you have only spoken to online, even if you believe you have established a relationship with the individual.
- Do not follow instructions from someone you have never met to scan a QR code and send payment via a physical cryptocurrency ATM.

- Do not respond to a caller, who claims to be a representative of a company, where you are an account holder, and who requests personal information or demands cryptocurrency. Contact the number listed on your card or the entity directly for verification.
- Do not respond to a caller from an unknown telephone number, who identifies as a person you know and requests cryptocurrency.
- Practice caution when an entity states they can only accept cryptocurrency and identifies as the government, law enforcement, a legal office, or a utility company. These entities will likely not instruct you to wire funds, send checks, send money overseas, or make deposits into unknown individuals' accounts.
- Avoid cryptocurrency ATMs advertising anonymity and only requiring a phone number or e-mail. These cryptocurrency ATMs may be non-compliant with US federal regulations and may facilitate money laundering. Instructions to use cryptocurrency ATMs with these specific characteristics are a significant indicator of fraud.
- If you are using a cryptocurrency ATM and the ATM operator calls you to explain that your transactions are consistent with fraud and advises you to stop sending money, you should stop or cancel the transaction.

The FBI Victim Services Division is responsible for ensuring that victims of crimes investigated by the FBI are afforded the opportunity to receive the notification and services as required by federal law and the Attorney General Guidelines for Victim and Witness Assistance. Victim Specialists are highly trained professionals who assess victims' needs to determine what types of services and resources will be most helpful. For more information, please visit www.fbi.gov/resources/victim-services.

If you believe you have been a victim of a cryptocurrency ATM or QR code scam, report the fraud to your local FBI field office. The FBI also encourages victims to report fraudulent or suspicious activities to the FBI IC3 at www.ic3.gov.

State of New Jersey
Commission of Investigation

BITCOIN ATMs

Scams, Suspicious Transactions and Questionable Practices at Cryptocurrency Kiosks

February 2021

State of New Jersey
Commission of Investigation

BITCOIN ATMS

Scams, Suspicious Transactions and Questionable Practices at Cryptocurrency Kiosks

SCI
50 West State St.
P.O. Box 045
Trenton, N.J.
08625-0045
609.292.6767

www.state.nj.us/sci

State of New Jersey

COMMISSION OF INVESTIGATION
50 WEST STATE STREET
PO Box - 045
TRENTON, NEW JERSEY 08625-0045
Telephone (609) 292-6767
Fax (609) 633-7366

February 2021

Governor Phil Murphy
The President and Members of the Senate
The Speaker and Members of the General Assembly

The State Commission of Investigation, pursuant to N.J.S.A. 52:9M-1 to -20, herewith submits its final report of findings and recommendations stemming from an investigation into the operation of privately owned automated teller machines that facilitate the purchase or sale of cryptocurrency.

Respectfully,

Joseph F. Scancarella
Chair

Robert J. Burzichelli
Commissioner

Kevin R. Reina
Commissioner

Rosemary Iannacone
Commissioner

TABLE OF CONTENTS

Introduction

The Commission initially launched an inquiry into the operation of privately owned automated teller machines (ATMs) in New Jersey based upon allegations suggesting their use in facilitating illicit financial activity and other questionable practices. Subsequent investigation revealed improprieties related to a specific type of emergent machine known as Bitcoin ATMs, or kiosks, that allow customers to buy or sell cryptocurrency.[1]

The machines, which look similar to traditional ATMs and are often located near their familiar counterparts in coffee shops, convenience stores and other retail outlets, enable users to quickly and easily conduct cryptocurrency transactions. Yet, unlike regular ATMs, there is no state regulation of their operation in New Jersey, and the federal laws that are supposed to protect against money laundering and other financial crimes are complex**,** can be difficult to interpret and are not always enforced.

The Commission examined hundreds of records subpoenaed from 30 businesses that operated or were associated with approximately 300 cryptocurrency kiosks in New Jersey over the last five years and found instances where the machines were used to effectuate financial scams and to orchestrate questionable transactions.[2] Some transactions appeared arranged in a way that enabled users to circumvent machine requirements to produce a valid form of identification or to avoid triggering specific federal currency reporting rules. In many instances, the transactions should have been flagged by operators as indicators of potential criminal activity and reported to the federal government but were not.

Not only did the Commission discover wide variability in the precautions operators take – or fail to take – to safeguard against fraud, the inquiry also found inconsistencies among the various companies in how the businesses function, the type of information they collect from customers and the purchase limits for users. Lacking any government-sanctioned criteria for operation, business owners set their own rules for how much cryptocurrency users can buy, for the percentage charged for transaction fees – some were as high as 24 percent – and for the type of personal identifying information required to complete a sale.[3] Many machines permit near anonymity on purchases of up to $900 worth of cryptocurrency by allowing users to provide only a cellphone number. Some require no identifying information at all.

While the value of Bitcoin – the first and most widely used cryptocurrency – has fluctuated wildly in recent years, it hit a record high in February, trading above $50,000 per unit. As Wall Street's enthusiasm for Bitcoin has grown, so has the market for digital currency businesses, including the machines that enable in-person purchases of it.[4] Major corporations, including Microsoft, AT&T, Overstock.com and even Starbucks, now accept Bitcoin as a legitimate form of

[1] The machines are also known as BTMs.
[2] The Commission subpoenaed records from businesses operating in New Jersey from 2015 to 2020. Not all of the companies were operating at the time of the publication of this report.
[3] The Commission found wide disparity in transaction fees charged on the machines with rates typically ranging from eight to 20 percent. The rates often fluctuate based on market conditions.
[4] Many kiosks allow the purchase of various types of cryptocurrency.

payment.[5] As for the machines, only a handful existed when cryptocurrency kiosks first appeared in the United States in New Mexico in 2014, but now there are more than 11,665 nationwide.[6] Not only are the machines simple to operate, but they also offer investors a turnkey business opportunity with relatively cheap start-up costs and little overhead. Practically anyone with enough money – approximately $3,200 to $8,000 – and an Internet connection can buy a machine, plug it in and start doing business.[7]

Some of the qualities that make the machines appealing to users – their ease of use, the completion of transactions in real-time, and the ability to maintain a certain level of anonymity – also make them ripe for exploitation and criminal enterprise, such as money laundering. In July 2020, the Justice Department dismantled an unlicensed ATM network run by an owner/operator who admitted laundering between $15 to $25 million from in-person exchanges and transactions at his Bitcoin kiosks in California. A former bank employee, the operator admitted he knowingly laundered dirty cash, intentionally failed to register the business with the federal government and did not implement safeguards, such as conducting customer due diligence or filing reports on suspicious financial activity.

Across the nation, financial institutions and government agencies at all levels are wrestling with how best to oversee cryptocurrency and the various businesses related to its use.[8] The federal government treats cryptocurrency kiosks the same as banks and other financial institutions, requiring they follow precautions intended to protect the world's financial system from illicit use and money laundering. It generally does not pursue cases against unregistered entities or those that otherwise ignore the rules unless the business is involved in other criminality. Among the states, New York has implemented the most far-reaching regulation of the industry by requiring any individual or company that engages in virtual currency business activity to obtain a BitLicense. Some industry operators have criticized New York's stringent licensing process as too lengthy, burdensome and costly, particularly for smaller companies. As a result, some cryptocurrency businesses have come to New Jersey, where nearly no rules apply.

With expectations that the worldwide demand for cryptocurrency and the various applications of associated technology – such as blockchain – will only escalate, the industry will present financially enticing yet thoroughly unregulated avenues for legitimate and corrupt businesses alike.[9] To guide the growth of this burgeoning industry, safeguard it for customers, and protect it from the intrusion of unsavory elements, state government must establish proper and effective oversight of it. It is also essential that any regulation of cryptocurrency-related commerce strike a balance between creating fair and reasonable standards that enable

[5] While Starbucks does not accept cryptocurrency as a direct form of payment, it utilizes third-party apps that use or convert it.

[6] The total number of machines in the U.S. as of November 2020, according to Cointelegraph, an industry website.

[7] Models with additional features that allow users to buy and sell cryptocurrency can cost up to $14,500.

[8] In New Jersey, cryptocurrency is legal and is subject to sales or use tax.

[9] Blockchain is a digital ledger of records, called blocks, stored together as a chain and is often publicly accessible. The technology can be used to store information related to many other types of transactions outside of cryptocurrency, such as medical data, banking and real estate. In August 2019, Governor Phil Murphy signed bill S-2297 into law creating the New Jersey Blockchain Initiative Task Force to study potential uses for the technology.

businesses in that sector to prosper while guarding against fraud and efforts to corrupt the system.

Legislation pending in both houses, A-2891/S-3132, would address many of the Commission's core issues and concerns raised in this report. Among other things, the "Digital Asset and Blockchain Technology Act" would require any digital asset business to obtain a license from the State Department of Banking and Insurance (DOBI).[10] In its current form, the bill would establish a regulatory apparatus for the growing industry that provides consumer protections while also enabling businesses to operate without overly onerous restrictions. Though it would regulate a broad spectrum of entities that operate within the digital asset sphere – not only kiosks – the State should also implement specific requirements specifically related to the machines. Further detail about this recommendation and other proposals for statutory and regulatory reforms is presented at the end of this report.

Background

The Commission's inquiry primarily focused on devices, known as "unidirectional" machines, that enable customers to purchase cryptocurrency but do not offer the option to cash it out.[11] Users simply insert cash into the machine, agree to pay a transaction fee, and within moments purchase cryptocurrency at the market rate. Instead of receiving actual money, customers get a code that effectively unlocks the value of the cryptocurrency. Almost all cryptocurrency transactions can be viewed on a shared public ledger, known as the blockchain. Once redeemed, the cryptocurrency is stored in the customer's "wallet," which exist in various formats. Digital wallets allow users to store and retrieve their cryptocurrency through a cellphone app or a computer. Among the most basic of storage methods for cryptocurrency are paper wallets, which are pieces of paper that contain a code and a "key" that essentially enables customers to unlock access to their cryptocurrency.

Unlike transactions made directly through online exchanges – a common way to purchase cryptocurrency – kiosk customers do not need to provide a credit card or link to a bank account. Some machines do not even require users to create an account to conduct a transaction. Whereas transactions on an online exchange may take days to complete, those conducted on the machines are immediate.[12] Industry operators maintain the kiosks appeal not only to customers who want to keep their personal information private but also to those with no bank account, the underbanked or those who operate mainly with cash, such as service industry workers.[13]

[10] The primary sponsors of A-2891 are Assemblywoman Yvonne Lopez and Assemblyman Andrew Zwicker, both D-Middlesex, and Assemblyman Joe Danielsen, D-Somerset. Sen. Nellie Pou, D-Passaic, is the sponsor of S-3132.

[11] Some machines enable users to both buy and sell cryptocurrency.

[12] Fraud verification procedures performed by the exchange or the account holder's bank often cause delays.

[13] More than 22 percent of adults either do not have a bank account or are underbanked, according to a 2019 study from the Federal Reserve. Underbanked refers to those who may have a bank or checking account but utilize alternative financial services such as money orders, cash checking services or pawnshop loans. The unbanked and underbanked are more likely to have low incomes, less education, or belong to a racial or ethnic minority group.

While still unfamiliar to many consumers, the kiosks represent a small but steadily growing industry in New Jersey. A Commission review of records identified more than $70 million deposited into machines for cryptocurrency purchases between 2015 and 2020. Like the cryptocurrency market at-large, the ATM business is volatile, with operators and machines frequently entering and leaving the state. Still, overall deposits have roughly doubled annually in each of the last five years.

No state law applies directly to kiosk operators/companies except for the mandate that the entity – just as any other business that operates in New Jersey – register with the Treasury Department. Outside of that, the sole oversight of digital asset companies occurs at the federal government level. Cryptocurrency ATM/kiosk companies are considered money services businesses, and as such, must register with the Financial Crimes Enforcement Network (FinCEN) of the US Department of the Treasury. FinCEN is responsible for administering the Bank Secrecy Act, which requires banks, financial institutions and businesses involved in transmitting or accepting convertible virtual currency to file reports on transactions that are potentially indicative of money laundering.[14] Under the law, these entities are obliged to monitor transactions and file a Currency Transaction Report (CTR) for every payment, receipt or transfer of currency or monetary instruments totaling in excess of $10,000 per day for each customer.[15] Operators are supposed to collect identifying information on customers they do business with and perform other due diligence under "Know Your Customer" (KYC) regulations.[16] Further, if unusual customer activity or questionable transactions are discovered, the operator is required to submit a Suspicious Activity Report (SAR) to FinCEN.[17]

Even though entities that disregard these requirements are flouting federal law, the Commission found registration and report filing violations were not actively policed for operators in New Jersey.[18] While US regulators have mostly taken a passive approach to oversight, federal law enforcement authorities have cautioned that as the use of cryptocurrency evolves and expands, so too will opportunities to exploit the technology and commit crime. An October 2020 report from the US Attorney General's Cyber Digital Task Force noted that the failure of entities, including kiosk operators, to comply with the Bank Secrecy Act and other legal requirements threaten the agency's investigative abilities and undermine public safety.[19]

[14] Convertible virtual currency refers to virtual currency that has a value equivalent to currency, acts as a substitute for currency and is therefore a type of value that substitutes for currency.

[15] 31 CFR § 1010.311

[16] The Bank Secrecy Act was amended under the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, also known as the Patriot Act, to require entities to provide customer identification information and monitor customers' habits and flag unusual activity.

[17] 31 CFR § 1022.320

[18] Under 18 U.S.C. § 1960, any person found guilty of operating an unlicensed MSB can face up to five years in prison. In addition, an unlicensed operator could also be liable for a civil penalty of $5,000 for each violation under 31 U.S.C. § 5330 and 31 CFR § 103.4.

[19] *Cryptocurrency: An Enforcement Framework* was the third and final report from the federal task force.

Key Findings

In its review of cryptocurrency machines, the Commission found areas of concern that legislators, law enforcement, and the public should be aware of as New Jersey considers measures to regulate elements of this swiftly expanding industry.

No ID Required

By permitting even a portion of transactions to occur anonymously, ATM operators leave the machines vulnerable to abuse by those who want to exploit the technology for nefarious purposes. Without capturing verifiable identifying information on its customers, their cryptocurrency transactions on the devices are virtually untraceable, which puts law enforcement at a distinct disadvantage when conducting investigations into suspicious activity.

A Commission analysis found the vast majority of companies that operate machines in New Jersey enabled users to conduct at least some transactions anonymously. Among the findings:

- Nearly 75 percent of the companies allowed certain transactions to proceed without requiring the user to present any information outside of a cellphone number.[20]
- More than half of those businesses permitted users to purchase up to $900 worth of cryptocurrency with only a cellphone number or no information at all.
- Security measures were stricter for larger purchases, with 87 percent of all companies requiring additional identification, such as Social Security number, ”selfies,” or tax ID for purchases exceeding $3,000.[21]
- Only 25 percent of businesses required buyers to provide a valid form of identification for every purchase.

Capturing cellphone information is an exceedingly unreliable method for verifying an individual's identity. Legitimate customers may use cellphones not registered under their own names but in an account in the name of a spouse or other relative. Individuals involved in criminal activity sometimes use pre-paid cell phones, known as “burners” or “throwaways” because they leave no trail back to the user. Typically purchased with cash, the phones require no proof of identification from the buyer and are disposed of once the pre-paid time expires. Unscrupulous individuals also often utilize so-called “burner numbers,” which are second phone numbers that can be purchased online and used on any cellphone. Just as it is with throwaway phones, purchasers of burner numbers select any available area code and phone number, making it difficult to trace back to a given individual.[22]

---

[20] The Commission reviewed machine settings and specific business practices for 16 ATM operators known to be operating in New Jersey in 2020.

[21] Many machines are equipped with cameras that take a photo of the user that are referred to as ”selfies.” Some require the customer to hold up a form of government identification in the photo.

[22] The Commission identified a handful of companies that prohibit the use of Voice over Internet Protocol (VoIP) phones to conduct machine transactions. VoIP uses an Internet connection instead of a landline or mobile network.

Even companies that appeared to be otherwise diligent about monitoring and reporting suspicious activities permitted purchases that necessitated the user to furnish only a cellphone number. The Commission uncovered examples in which customers conducted several smaller transactions in a short time frame, enabling the users to dodge machine requirements to produce a valid form of identification for larger purchases. The smaller transactions also often skirt the $2,000 threshold that triggers the operator to file a SAR. The failure to capture identifying information on users for *all* machine activity means that even operators that are appropriately watching the transactions and informing FinCEN of questionable events do not truly know their customers.

A North Jersey-based operator told the Commission the company routinely monitored transactions and filed the appropriate reports to federal authorities if any activity appeared unusual. The company also utilized cameras on the machines to monitor customer activity. But the company knows nothing about customers who make purchases of less than $800 – outside of the cellphone number supplied by the user – a practice that effectively undermines its efforts to conduct thorough customer due diligence. The operator testified the company appropriately filed SARs after machine photos showed the same individual conducted a series of $800 transactions. However, the report would have provided little useful information to law enforcement authorities due to the lack of reliable identifiers for the customer.

Digital Mint, a larger Chicago-based company with three dozen machines in New Jersey, decided in 2016 to require customers to provide identification for all transactions after an internal audit found cellphone data was not adequate to meet FinCEN requirements. Although some customers initially complained and business briefly dropped off, those setbacks had no long-term impact on the company's bottom line, according to sworn testimony from its co-owner.

Questionable Compliance

The Commission found wide disparities among the 30 businesses operating cryptocurrency kiosks related to registration with state and federal agencies as well as their implementation of anti-money laundering controls. While most entities properly registered their business with the State of New Jersey, nearly a third failed to register to operate here legally.[23] In addition, more than a third of the companies did not register with FinCEN as money services businesses.[24]

Of the non-compliant entities, some willfully disregarded requirements to register their businesses and made no effort to monitor transactions or to implement practices that enable operators to know their customers. Others claimed total ignorance of the federal mandate to file SARs or report activity that could indicate money laundering. Moreover, some owners/operators

[23] In New Jersey, a business can be voided or revoked for the failure to file annual reports for two consecutive years or for the failure to file corporation business taxes.

[24] Not every business that did not register with the State also failed to register with the federal government. Six companies never filed with the State or FinCEN.

appeared to lack even a basic understanding of how the machines operated and insisted the manufacturer took care of anti-money laundering reporting obligations.

In sworn testimony before the Commission, Noel Harvey, the owner/operator of six machines in Bergen, Hudson and Morris counties, acknowledged he never registered Crypto Cash ACM – the name used for his kiosk business – or its parent company, SEVEC LLC, with FinCEN.[25] He never filed paperwork to flag questionable transactions or conducted customer due diligence either, claiming the manufacturer handled those matters. During his testimony, Harvey appeared unfamiliar with rudimentary procedures for the machines. He admitted being aware of financial schemes conducted through the company's devices but did not report the incidents to law enforcement. He also did not know whether certain transactions required the user to submit a phone number. When Commission counsel asked if he filed state or federal taxes for the business, Harvey exercised his constitutional right of protection under the Fifth Amendment against possible self-incrimination.

A review of transactions conducted at four of Harvey's terminals between April and September 2019 revealed several instances of transactions with purchases exceeding $10,000 – occasions that should have resulted in the filing of a report alerting FinCEN to questionable and possibly illicit activity. On one of those occurrences, a series of ten transactions – each for $1,000 that were sent to the same wallet – occurred in the span of a few minutes. The transactions appeared arranged in a way to evade the $10,000 daily customer threshold that triggers the filing of a CTR. At the very least, a vigilant operator should have alerted FinCEN that the purchases appeared suspicious. But that never happened because at Harvey's machines, identifying details about customers were not routinely collected, transactions were not reviewed, and no information was reported to FinCEN. Harvey testified that he did not know what, if any, identification the user was asked to provide for those purchases.

Harvey testified his initial exposure to the industry came from attending a cryptocurrency conference held in 2017 by a company later shut down by the Securities and Exchange Commission for running a pyramid scheme. Outside of that, his knowledge of the ATM business came from watching YouTube videos and from paid consultant Frank Robertson – a seven-time convicted felon with a long history of financial-related crimes who once co-owned a business, 2Nickles, that operated a handful of machines in North Jersey that were never registered with the state or FinCEN. Recently convicted of federal fraud charges, the Commission found evidence Robertson is back in the ATM business unlawfully operating two machines in Hudson County.

In October 2019, when SCI agents visited the gas station where one of the machines is located, a station employee identified Robertson as the individual who placed the kiosk there and serviced it. Robertson's contact information appeared at the top of a contract between an entity called Near By Coins ACM and the store owner to house the terminal. While the agreement was unsigned, the owner told investigators Robertson paid him $200 a month to lease the space.

[25] Records reviewed by Commission staff indicate SEVEC subsequently registered with FinCEN in September 2020, several months after Harvey's testimony before the Commission. Harvey previously registered SEVEC LLC, which operated as a parking company, as a business in New Jersey, but the company remains in suspended status due to the failure to pay the annual fee.

Meanwhile, there is no record of registration for the business with either the State of New Jersey or FinCEN.

When asked about his cryptocurrency-related activities during sworn testimony before the Commission, Robertson refused to answer questions concerning these matters, citing his Fifth Amendment privilege against self-incrimination. During the investigation, the Commission obtained evidence indicating certain operators, including Robertson and Harvey, worked under the belief that the machines – not the operator – took care of flagging questionable transactions and reporting such activity to authorities.

General Bytes, one of the largest manufacturers of Bitcoin kiosks and the company that sold machines to both Robertson and Harvey, told the Commission the devices it sells do not perform any anti-money laundering compliance functions. In a September 2020 email to the SCI, the owner of the Czech Republic-based company further wrote:

> *Yes, we instruct customers to consult with their local lawyers and accountants what their responsibilities are. Giving other, a more specific advises [sic] may mislead customer. We are ATM manufacturer. We sell ATMs all over the world. We do not want to pretend that we are competent to give legal advises [sic] to companies. Crypto-currency regulation is different in every country and changes every 6 months. We believe that our customers understand that they need MSB licenses and similar and know what their responsibilities are.*

While some operators knowingly violated the rules, others professed ignorance concerning their obligations to register their business with FinCEN and comply with anti-money laundering mandates. The owner/operator of a lone machine in Fort Lee, who at the time had been in business less than a year, claimed to be completely unaware of the need to register with the federal government as a money services business until he was advised of this requirement by Commission agents.[26] In response to a Commission subpoena requesting information on whether he had discovered or reported any suspicious financial activity on his machine, the owner/operator wrote:

> *This is actually the first time I became aware of SARs and its purpose. As reporting any SARs is required to be submitted within a specific timeframe [sic] I have not experienced any recent fraud or scam. However moving forward, I will document and report any suspicious activity to FinCen [sic].*

Similarly, the owner/operator was unfamiliar with currency transaction reports.

> *Unfortately[sic], same as SARs, I did not have any knowledge CTRs and it's [sic] purpose. Moving forward, I will document and report any currency transactions in excess of $10,000 to FinCen [sic].*

[26] The owner/operator has since registered with FinCEN as an MSB and hired a certified anti-money laundering specialist and fraud examiner to advise his business.

A Commission review of transactions at the machine between July 2018 and June 2020 revealed that $206,000 flowed through the device during that time without any monitoring by the operator to comply with KYC and anti-money laundering laws.[27] Equally troubling, no identifying information was captured for any of the customers in those transactions.

Based on the Commission's review, it is clear that operators in New Jersey are not consistently or committedly complying with reporting mandates and that absent greater conformity, the kiosks remain vulnerable to abuse and criminal intrusion. These findings reinforce warnings from the Justice Department that businesses that avoid compliance with anti-money laundering standards and KYC requirements provide opportunities for criminals to hide their illicit financial gains from regulators and criminal investigators.

Fraudulent Schemes

In addition to their use as vehicles for questionable transactions, criminals also utilize cryptocurrency kiosks to carry out various types of fraudulent schemes.[28] The Commission uncovered numerous instances where unwitting victims were duped into sending cryptocurrency to unknown wallets through the machines, including some schemes that resulted in the loss of tens of thousands of dollars. Cryptocurrency transactions are irreversible, leaving victims with no way of recovering the lost funds.

By monitoring activity at the machines, diligent operators can halt schemes from progressing, or at the very least, flag suspicious transactions and alert federal authorities to activity potentially indicative of further misconduct. To their credit, some ATM companies have developed proactive strategies to inform customers about potential fraud and required users to review a disclaimer outlining the risks associated with cryptocurrency before commencing any transactions. Others have placed stickers on the machines warning customers of scams and urged users to alert operators to requests from third parties to send cryptocurrency to them. The Commission identified several companies that required customers to certify the wallet where the virtual currency was sent belonged to them and not someone else. Some operators, such as BelcoBTM, have cultivated employees in the stores that house machines to keep an eye out for suspicious activity or unfamiliar users.

Companies that discover individuals using their machines to engage in inappropriate activities also have the ability to ban those customers from the kiosks or to block certain wallets. An SCI review of company records found more than 900 customers or wallets that were either banned or blocked by 10 companies with kiosks in New Jersey. Operators banished individuals

[27] The machine is unlike most of the terminals located in New Jersey as it permits both the purchase and sale of cryptocurrency.

[28] The Justice Department has also linked the kiosks to unlawful conduct by drug dealers, credit card schemers and prostitution rings.

from their machines for various reasons, including the utilization of multiple wallets, using Bitcoin obtained on the machine to fund Darknet purchases or for an association with a scam.[29]

Among the schemes identified by the Commission:

- Cryptocurrency kiosks were utilized to carry out a scam that duped multiple victims into spending a total of more than $600,000 to buy vehicles advertised for sale on eBay but did not really exist. Under the scheme, purchasers wire transferred money intended for the vehicle acquisition to a particular bank account. After receiving the money, an individual working for the scammer would take the funds, purchase bitcoins through various kiosks in New York City and New Jersey, and then send it to designated wallets controlled by the scam artists. From October 2016 to March 2017, this individual purchased more than $170,000 in bitcoin at a Lyndhurst kiosk alone. Law enforcement learned about the scheme after a victim contacted a bank where money was wired and reported never receiving a vehicle. Ultimately, the New Jersey State Police arrested and charged the individual with various crimes, including theft by deception, money laundering and deceptive business practices.

- In April 2019, a caller identifying himself as both an agent with the Federal Trade Commission and a U.S. Marshal informed the victim that her identity had been stolen. The caller claimed two properties in Texas that authorities suspected were linked to money laundering activity and drug trafficking were purchased in the victim's name. In addition, the caller told the victim her Social Security number was used to open four bank accounts. The scammer warned the victim that all her bank accounts would be frozen pending further investigation, but she could “prove her innocence” if she moved money from her bank accounts, converted it to cryptocurrency and transferred it to an allegedly secure federal account already set up. The victim had 40 minutes to drain her accounts and visit seven different cryptocurrency kiosks in Bergen, Essex and Passaic counties to deposit the money into a secured “federal account.” After completing the final transaction at an ATM in Clifton, a store associate approached the victim and asked where she was sending the money. The store worker had received a call from an employee of the machine's operator, who was aware of the prevalence of scams and knew the woman was not a regular customer based on real-time monitoring of the transactions. In total, the woman lost $12,000 in the scam.

- In July 2019, a customer contacted the owner/operator of a Fort Lee machine to report a fraud in which an unknown caller requested the victim to use the terminal to send $8,000 in bitcoin, broken down into smaller increments of $500, to a specific wallet.[30] After sending the money, the victim realized it was a fraud and reported the incident to the owner/operator.

[29] The Commission found two ATM companies banned a Staten Island man from using their machines after discovering he purchased bitcoin that was later sent to offshore gambling websites.

[30] The scammer likely requested the victim to purchase the $8,000 in smaller amounts in order to avoid triggering KYC reporting requirements.

- In September 2019, a victim reported receiving a call from a caller identified as a Public Service Electric and Gas employee who demanded payment for an outstanding debt that, if not resolved, would result in legal action against the target. The caller instructed the victim to purchase $450 in bitcoin at the Fort Lee cryptocurrency machine and send it to the address provided by the scammer. After completing the transaction, the victim grasped the scheme and contacted the owner/operator inquiring about whether the lost funds were recoverable, but was told all transactions are irrevocable.

Recommendations

Under current laws and regulations, New Jersey has no authority over the burgeoning cryptocurrency industry. As demonstrated by the findings in this report, the lack of oversight of machines that enable users to purchase significant amounts of cryptocurrency practically anonymously renders them vulnerable to abuse by bad actors who seek to exploit the technology for illicit purposes. Without any state regulation of their operation, no protections exist for consumers unfamiliar with the fast-moving terrain of cryptocurrency transactions and fall victim to scams. Further, there are no standards to ensure operators of these businesses function in a reliable, consistent and transparent manner.

As indicated earlier in this report, pending legislation, A-2891/S-3132, would address a number of the concerns raised by the Commission by creating a licensing mechanism for individuals who engage in a digital asset business activity, including cryptocurrency kiosks.[31] An applicant for licensure would be required to disclose any criminal convictions or pending criminal charges against either the business's primary operator or top officers. Further, it also would require the disclosure of any ongoing litigation, a bankruptcy filing within the prior ten years or a license revocation or suspension in another state. Under the measure, any individual who operates a digital asset business without a license would face a fine of $500 per day.

To protect consumers, the bill requires the disclosure – "in readily understandable language" – of the terms and conditions of a customer's account with the business regarding fees or charges, potential risks and any protections and securities in place. A customer would need to agree to the terms set out in the disclosure before any transaction or digital asset balance inquiry commenced at a kiosk.

In addition to enacting this legislation, decision-makers should consider – either as an amendment to the bill or by department regulation – expanding the period for record retention beyond the one year proposed, and instead applying the same standard that pertains to businesses in the banking industry. In New Jersey, banks and financial institutions must retain records of accounts, including transactions, for six years.[32] Limiting access to only a twelve-month window could constrict the ability of law enforcement and regulators from obtaining a larger

[31] The legislation would also honor licenses held by operators or businesses in a state with a reciprocity agreement with New Jersey.
[32] N.J.S.A. 17:16W-3

volume of information needed to investigate incidents of suspicious financial activity. At a minimum, the criteria should match those under the Bank Secrecy Act, which requires money services businesses to retain records related to transactions for five years.

While the proposed legislation requires disclosure of an applicant's criminal history, the Commission recommends the DOBI Commissioner apply greater scrutiny to any individual convicted of a crime of moral turpitude involving dishonesty, fraud or deceit within the past ten years. During the inquiry, the Commission identified two individuals with recent federal convictions for financial-related crimes whose ATM companies engaged in various questionable business practices.

Concerning the operation of the machines, it should be mandated that all machine customers provide a valid form of government-issued identification with a photo before any transaction can proceed. Requiring IDs for all purchases ensures that every transaction on a device is traceable to a specific individual. Without identifying information on users, law enforcement's investigative capabilities remain hamstrung when probing suspicious transactions and potential links to criminal activity. The Commission identified several cryptocurrency businesses that have taken the lead in this area and already require customers to provide government-issued IDs for all transactions.[33]

[33] In addition to Digital Mint, the Commission found three other companies with machines in New Jersey – Coinlinx, Coinsource and Byte Federal – all require customers to present valid government-issued identification before a transaction can proceed.

ATHENA BITCOIN

Avoid these Bitcoin Scams

Read our article on the most common Bitcoin scam here.

Financial scams involving digital currencies like Bitcoin are a growing component of the overall fraud universe that still involves gift cards, Western Union/MoneyGram, money orders, and bank wires.

> **Scammers are looking to say and do anything to convince you of a urgent need to pay through Bitcoin, and they will often "helpfully" point out nearby ATMs where you can follow their commands.**

Scam artists like Bitcoin because transactions cannot be cancelled, reversed, or otherwise refunded once made.

Athena receives numerous reports of fraud per month, so we want to share much of what we've learned to look out for when it comes to Bitcoin, digital currency, and physical cash kiosks.

Bitcoin Scams to Avoid

Warning: Scam artists can *spoof* or fake ANY telephone number or email address they want!

Do NOT rely upon caller ID at all to determine who is calling.

Impersonation scam - Tech companies, Banks, and Utilities

Tech Support / Bank Impersonation Scam

This has been the most common scam of 2022!

A pop-up message will appear on your computer telling you that it has been hacked and you need to call a Microsoft (or Apple / Google) support number for assistance. The pop-up is often accompanied by a loud warning sound.

DO NOT CALL ANY NUMBER THAT APPEARS IN A POP-UP!

Scammers place these messages on victim's PCs and tablets in the hopes that they will call the scammer impersonating a major tech company. The scammer will often have you download remote access software that can potentially view and access anything on your PC, including bank accounts. Ultimately, the scammer's goal is to convince you that something is wrong with your bank and ask you to withdraw physical cash to "secure it" through a Bitcoin ATM. Often multiple scammers are involved in each incident impersonating the tech company and an agent from your bank.

The solution to this one is easy: **Always call out to your bank using the number on your bank statement or visit a branch of your bank in person to verify the situation!** Bank personnel will never call you and ask you pull out cash.

Seek professional computer repair services to remove any malware on your PC, tablet, or phone.

Utility Impersonation Scam

Someone pretending to be from your utility company (usually electric) will call or email you to claim you are late on a bill. They will then threaten to shut off your electric or other utility service if you don't pay immediately in bitcoin.

Just HANG UP, take a breath, and find the number for your actual utility company who you may call for the real status of your account.

Scammers count on you being panicked and willing to follow their direction without question. Don't talk to them and don't call any numbers they give you. Refer to your utility bill or website for actual contact information. See also: www.utilitiesunited.org

ATHENA BITCOIN

Impersonation scam - Government

Threat of Arrest and "Protect Your Savings" Scams

A very common form of the impersonation scam is where you will receive a call supposedly from a government agency. This could be the Social Security Administration, U.S. Marshals, FBI, Department of Homeland Security, Immigration and Customs Enforcement, local police, and more. The scammers will often tell you that you are in trouble and are about to be arrested, or that you are connected with criminal activity and you need to help them clear your name / SSN.

Regardless of the setup, the scam always ends with you taking cash out of your bank and putting it into a "government kiosk" (really a Bitcoin ATM). The perpetrators often have another scammer call you pretending to be a different person to "confirm" the fraud.

This particularly awful fraud has impacted many.... JUST HANG UP and block the number that is calling you. Call out to or visit someone you trust, instead, for support and advice!

Again, never send bitcoin to anyone pressuring you to do so.

IRS Scam

Some government scams take the form of demands from the IRS to pay debts owed. The scammer can contact you through any communications method, including phone calls. This type of scam can be potentially very costly for the victim, including a high risk for stealing sensitive personal information. The scammer may threaten you and will sometimes provide details to pay via bitcoin.

Of course, **Uncle Sam does not *yet* accept bitcoin. Never pay supposed IRS debts via an ATM!**

Other commonly reported forms of fraud

Money Mule Scam

- This is **any** situation where you are receiving money from someone else (physical cash, personal or cashier's checks, bank-to-bank transfers, Venmo/Paypal, bank-to-bank transfers) and purchasing bitcoin on their behalf. This *may* also involve a "cut" or fee that you get to keep yourself for your "service".

  This situation is **highly dangerous** and will subject you to further prosecution for participation in money laundering. The likely reason someone would pay *you* to purchase bitcoin for them is because they want to obscure the source of past theft, fraud, or other criminal behavior.

  Do not help them!

Scams of the Heart

- **Relationship scam**: Victim believes they are in a relationship with someone they either rarely meet or never meet and is often in another country. Scammer asks them to help pay for urgent expenses, including costs of traveling to see the victim, equipment for a business, customs fees, medical bills, and so forth. Bitcoin is especially applicable here since it is often used for cross-border payments. Unfortunately, **relationship scams can go unnoticed for quite some time and result in a devastating betrayal.**
- **Grandparent scam**: Victim is contacted by a supposed relative, often a grandchild, cousin, niece, or nephew who needs bail money or is otherwise in urgent trouble. After briefly describing the problem the scammer cuts off communication except for payment instructions, intending to panic the victim. **This scam particularly impacts the elderly.** We would suggest taking your time and verifying the story with other relatives before sending any money.

Investment Scams

As always...

> **If it sounds too good to be true, it almost always is!**

- **Social Media** (Facebook, Instagram, Tiktok, Twitter, Discord, Telegram, etc.): Victims are contacted by "friends" through social media platforms and told about high earnings through some investment site / app or via a particular investment advisor. The "friend" accounts are often hacked, and the scammers target everyone connected to the hacked account. Other solicitations may come through direct messages that allow one-on-one conversations. Scammers direct you to send money – often via digital currency – to a third-party or to a legitimate-looking website. You may even be able to login and track your "earnings" on this website, but the entire thing is fake. As soon as you request a withdrawal, the website will request payments of fees and taxes using new money. Many would-be investors end up paying these fees and wind up losing even more money.

  Always call your friend to verify any investment situation and never allow social media ads or direct messages to strongly influence your investing decisions.

- **Ponzi** / **Pyramid schemes**: Victims will see ads for investment programs promising unusually high rates of return. Claims are often made to behind-the-scenes forex or digital trading. Many also advertise their own new token as being a "better Bitcoin" where you can get in on the ground floor– the implication being that it will, too, experience Bitcoin-like rates of explosive growth. Unfortunately, virtually all of these are scams. The investment principal from later investors are used to pay out the earlier investors until the whole scheme collapses. **One of the biggest warning signs are promises to pay a specific percentage of earnings daily or weekly.** Pyramid schemes are often tacked on in the form of referral bonuses. They rely upon ever expanding downstream networks of distributors to promote the scheme and are also doomed to collapse.

  Bitconnect is a famous example of a Ponzi and Pyramid scheme from 2017/18 whose token lost 99% of its value following state regulatory pressure (1,2,3). Other notable scams include Onecoin, Gladiacoin, and USI-Tech.

  Ponzis will always exist in one form or another and wreck many naive investors' lives. Don't let it happen to you.

Fake Income Scams

- **Check cashing scam:** This category also includes **fake jobs or interviews.** Someone remote will offer to pay you via check (sometimes other forms) and expect you to send bitcoin to another destination for some believable reason. Excuses include sending money to clients, purchasing a wardrobe, or paying for transportation. Not only is this potentially money laundering, but most likely you will see the original check bounce and only *you* will be responsible for the lost cash or bitcoin. In short, if someone is sending you money just so you can send money somewhere else, be very suspicious.
- **Advance Fee scam:** Someone contacts you to tell you that you've been awarded a grant, lottery winnings, or are due to receive an inheritance. The scammers often impersonate governments or lawyers. To receive this award, **you have to first send bitcoin** through an ATM to pay for the "processing fees" or "taxes". The scammer will then disappear and leave you high and dry. Never pay governments or lawyers via Bitcoin / digital currencies, especially if they are promising you something or contact you out of the blue.

Fake Merchandise Scams

These are listings for "great deals" on typically high-value items on Craigslist, eBay, OfferUp, Amazon, and other places where individuals can post ads. They are most likely selling....

- **Apartment rentals / down payments:** Scammers either point to legitimate listings on Airbnb or other listing sites, create copycat websites that look like these sites, or possibly create their own fake listings just to lure people into a conversation outside of a legitimate rental website. Once the victim communicates with them **the scammer will give the victim instructions via email** or some other channel to pay for their "reservation" or "down payment" with bitcoin. We've also seen EasyRoommate and HomeAway affected by this.
- **Tickets for concerts or other events:** Scammers will list on Craigslist or other individual ad sites fake or non-existent concert tickets sold for bitcoin. As is usual in these cases, the scammer will just disappear, and you will be out hundreds of dollars. We've seen **theme park** tickets also the subject of this scam.
- **Used cars / eBay Motors scam:** The scammer will post a used car for a very low price on Craigslist, reusing photos and data from some older or legitimate listing elsewhere. The scammer will often tell a personal story involving the death of a family member or military deployment forcing them to sell the car. They will also promise to ship the car to the buyer, offering no way to meet in person. **What's worse is that they will go to great lengths make their emails look real,** but the car doesn't exist, eBay has no knowledge of it, and the victim will simply lose their money.

eBay, Amazon, Airbnb, Ticketmaster, and many other major retailers DO NOT *yet* accept bitcoin!

...and if they did, they would do so only through their own secure websites.

Unsure about a payment? **STOP! ...and give us a call (312-690-4466) or message.** We can't determine if your destination is legitimate, but we can help you assess the risk that it may not be. Likewise, anyone can call out to the AARP Fraud Watch helpline for advice and support: **877-908-3360** (Mon-Fri 7:00 am – 11:00 pm ET)

March 29, 2018

Avoid these Bitcoin scams!

Patrick · Scams

New alert page for the most common scam that we see!

Jump to Fraud List

Operating over 100 ATMs across North and South America means that Athena is the gateway for tens of thousands of customers to the world of Bitcoin and other digital currencies. While we help customers every day get the coins they want and need, **some customers end up unwittingly victims of fraud perpetuated by con artists**. We've issued scam warnings in the past (1,2,3), and even broke news about one "hurricane" scam in 2017, but we wanted to provide a more comprehensive list of situations you should look out for.

It's important to note that these are scams that have existed for much longer than Bitcoin has been around. Most have been adapted to take advantage of this new payment form, but have previously and *are still* conducted using gift cards, Western Union/MoneyGram, money orders, or even bank wires. **Scammers using Bitcoin will often "helpfully" point out nearby ATMs from which you can send them money.** They like Bitcoin because transactions cannot be cancelled, reversed, or otherwise refunded once broadcast...

— Bitcoin Scams to Avoid —

Click on the scam type below to read full descriptions from Fraud.org and other great resources.

Warning: Scam artists can *spoof* or fake ANY telephone number or email address they want! Do NOT rely upon caller ID at all to determine legitimacy.

Impersonation scam - Government:

- IRS scam: Many government scams take the form of demands from the IRS to pay debts owed. The scammer can contact you through any communications method, including phone calls. This type of scam can be potentially very costly for the victim, including a high risk for stealing sensitive personal information. The scammer may threaten you and will sometimes provide details to pay via bitcoin. Of course, **Uncle Sam does not *yet* accept bitcoin. Never pay supposed IRS debts via an ATM!**
- Social Security scam: Another form of the impersonation scam is where you will receive a call supposedly from the Social Security Administration, often claiming that your SSN has been

- **Social Security scam:** Another form of the impersonation scam is where you will receive a call purposedly from the Social Security Administration stating that your SSN has been "suspended" or otherwise part of some criminal activity. *They will probably threaten jail time* and then demand payment via a local Bitcoin ATM. The perpetrators often have another scammer call you from your "local police" to corroborate the story of the first. **This particularly awful fraud has impacted many >>> JUST HANG UP and CALL US immediately!** Again, never send bitcoin to anyone pressuring you to do so.

Impersonation scam - Utilities:

- **Threats to shut off service:** Someone pretending to be from your utility company (usually electric) will call or email you to claim you are late on a bill. They will then threaten to shut off your electric or other utility service if you don't pay immediately in bitcoin. **Just HANG UP, take a breath, and find the number for your actual utility company who you may call for the real status of your account.** Scammers count on you being panicked and willing to follow their direction without question. Don't talk to them and don't call any numbers they give you. Refer to your utility bill or website for actual contact information. See also: www.utilitiesunited.org

Fake Merchandise Scams (more info)

These are listings for "great deals" on typically high-value items on Craigslist, eBay, OfferUp, Amazon, and other places where individuals can post ads. They are most likely selling...

- **Apartment rentals / down payments:** Scammers either point to legitimate listings on Airbnb or other listing sites, create copycat websites that look like these sites, or possibly create their own fake listings just to lure people into a conversation outside of a legitimate rental website. Once the victim communicates with them **the scammer will give the victim instructions via email** or some other channel to pay for their "reservation" or "down payment" with bitcoin. We've also seen EasyRoommate and HomeAway affected by this.
- **Tickets for concerts or other events:** Scammers will list on Craigslist or other individual ad sites fake or non-existent concert tickets sold for bitcoin. As is usual in these cases, the scammer will just disappear, and you will be out hundreds of dollars. We've seen **theme park** tickets also the subject of this scam.
- **Used cars / eBay Motors scam:** The scammer will post a used car for a very low price on Craigslist, reusing photos and data from some older or legitimate listing elsewhere. The scammer will often tell a personal story involving the death of a family member or military deployment forcing them to sell the car. They will also promise to ship the car to the buyer, offering no way to meet in person. **What's worse is that they will go to great lengths make their emails look real**, but the car doesn't exist, eBay has no knowledge of it, and the victim will simply lose their money.

eBay, Amazon, Airbnb, Ticketmaster, and many other major retailers DO NOT *yet* accept bitcoin!

...and if they did, they would do so only through their own secure websites.

Fake Income Scams

- **Check cashing scam:** This category also includes **fake jobs or interviews.** Someone remote will offer to pay you via check (sometimes other forms) and expect you to send bitcoin to another destination for some believable reason. Excuses include sending money to clients, purchasing a wardrobe, or paying for transportation. Not only is this potentially money laundering, but most likely you will see the original check bounce and only *you* will be responsible for the lost cash or bitcoin. In short, if someone is sending you money just so you can send money somewhere else, be very suspicious.
- **Fake grant scam:** Someone contacts you to tell you that you've been awarded a grant or some other giveaway, usually by a government agency. To receive this award, **you have to first send bitcoin** through an ATM to pay for the "processing fee". They will disappear and leave you high and dry. Other variants ask you for checking account details.

Scams of the Heart

- **Relationship scam:** Victim believes they are in a relationship with someone they either rarely meet or never meet and is often in another country. Scammer asks them to help pay for urgent expenses, including costs of traveling to see the victim, equipment for a business, customs fees, medical bills, and so forth. Bitcoin is especially applicable here since it is often used for cross-

EXHIBIT E to Complaint

- **Relationship scam**: Victim believes they are in a relationship with someone they either rarely meet or have never met and [illegible] help pay for [illegible] expenses, including costs of traveling to see the victim, equipment for a business, customs fees, medical bills, and so forth. Bitcoin is especially applicable here since it is often used for cross-border payments. Unfortunately, **relationship scams can go unnoticed for quite some time and result in a devastating betrayal.**
- **Grandparent scam**: Victim is contacted by a supposed relative, often a grandchild, cousin, niece, or nephew who needs bail money or is otherwise in urgent trouble. After briefly describing the problem the scammer cuts off communication except for payment instructions, intending to panic the victim. **This scam particularly impacts the elderly.** We would suggest taking your time and verifying the story with other relatives before sending any money.

Investment Scams

This category involves some of the most common types of scams and those that are the hardest to recognize (before it's too late), but there are still signs...

- **Ponzi / Pyramid schemes**: Victims will see ads for investment programs promising unusually high rates of return. Claims are often made to behind-the-scenes forex or crypto trading. Many also advertise their own new token as being a "better Bitcoin" where you can get in on the ground floor--the implication being that it will, too, experience Bitcoin-like rates of explosive growth. Unfortunately, virtually all of these are scams. The investment principal from later investors are used to pay out the earlier investors until the whole scheme collapses. **One of the biggest warning signs are promises to pay a specific percentage of earnings daily or weekly.** Pyramid schemes are often tacked on in the form of referral bonuses. They rely upon ever expanding downstream networks of distributors to promote the scheme and are also doomed to collapse.

  Bitconnect is a famous example of a Ponzi and Pyramid scheme from 2017/18 whose token lost 99% of its value following state regulatory pressure (1,2,3). Other notable scams include Onecoin, Gladiacoin, and USI-Tech.

  > **Ponzis will always exist in one form or another and wreck many naive investors' lives.**
  >
  > Don't let it happen to you.

- **Initial Coin or Exchange Offerings (ICOs/IEOs)**: ICOs/IEOs are the initial sale of a new token to the public, analogous to an Initial Public Offering for stock. Normally taking the form of ERC-20 tokens created on the Ethereum network, ICOs became a popular and novel way to raise funds in 2017. While some forms of ICOs may be legitimate, the legal consequences surrounding these investments are still poorly understood, with many of them likely to be considered securities by the SEC. Regardless of their regulatory status, scammers make use of ICOs in attempted "pump and dump" schemes by the hundreds. It was widely reported that nearly half of 2017's ICOs have already failed. **Please do considerable research before participating in any ICO**, and don't feel pressured by limited-time token sales.

Unsure about a payment? **STOP! ...and give us a call (312-690-4466) or message.** We can't determine if your destination is legitimate, but we can help you assess the risk that it may not be.

Tagged: ponzi, pyramid, ICO, ebay, IRS, Airbnb, romance, grandparent, fake check, concert ticket, used car, scam, fraud

❤ < Share

Newer Post
How to use a Paper Wallet

Older Post
Not seeing your Litecoin or Bitcoin Cash transaction? Here's how to find your payment status...

FRAUD ALERT

Imposter scams are the most common Bitcoin fraud that we see!

Imagine being in a panic thinking that you will be arrested or that money is about to be drained out of your bank account?

Imagine having someone on the phone with you for *hours* making sure you obey their instructions?

Thousands of people each year don't have to imagine....

"We will have to issue an arrest warrant in your name...."

– Common variant of the social security / government imposter scam

If...

- You receive a call or message saying that something is wrong with your bank, social security number, or that you are connected with a crime, **hang up or don't call back.**
- You receive a popup alert on your computer screen, **do not call the number presented**
- You are in a live call with someone who is requesting that you do something with your money, **hang up and research this on your own!**
- You are concerned about your social security number, ***dial out* to your local field office or the national number: 800-772-1213**
- You are concerned that someone has stolen your identity, please visit **IdentityTheft.gov**

02:28

Don't...

- **Withdraw physical cash** from your bank under the instructions of someone else, regardless of the reason given.
- **Make irreversible payments**, including bank wires, gift cards, physical cash, or **Bitcoin transactions**.
- Assume that the number on your Caller ID has anything to do with who is actually calling – numbers can be easily faked!
- Panic! Always hang up on whomever is distressing you and *take your time* to thoroughly analyze the situation.
- Go it alone! No matter what you are told, consult a trusted friend or family member (or visit your bank) to get a second opinion. The scammers want to *isolate you* and keep you from finding sound advice.

Do...

- READ our **scam warning page** at least once!
- Report any scam attempt to the FBI's **Internet Crime Complaint Center** or call **VictimConnect** at 855-484-2846 (Mon-Fri 9:00 am – 5:00 pm ET)
- Include any Bitcoin address you were given by the scam artist in your reports to any agency, as Bitcoin addresses can be traced back to the perpetrators.
- SHARE this warning page with as many people as you can!

  Other helpful sites:

  - **https://www.ssa.gov/scam/**
  - **AARP Fraud Resource Center**
  - **https://www.ftc.gov/imposter**
  - **https://www.justice.gov/elderjustice/senior-scam-alert**

It's NOT enough to protect just yourself from fraud ...

Please help spread the word to your friends and family about the methods used by these scam artists.

The best way to prevent these types of fraud, nationwide, is through **education** and **awareness** before they happen.

United States Senate
WASHINGTON, DC 20510

September 11, 2024

Matias Goldenhörn
Chief Executive Officer
Athena Bitcoin
1 SE 3rd Avenue Suite 2740
Miami, FL 33131

Dear Mr. Goldenhörn:

We write to call on you to take immediate action to address troubling reports that your Bitcoin ATMs (BTMs) are contributing to widespread financial fraud against elderly Americans. Cryptocurrencies, including Bitcoin, have long been associated with criminal activity. The relative anonymity and irreversibility of cryptocurrency transactions has made them particularly attractive to fraudsters. As companies like yours have staged BTMs in a variety of businesses—sometimes even paying businesses to host your BTMs—there has been a marked increase in Bitcoin scams impacting elderly Americans. In light of these troubling reports, Athena Bitcoin must take all necessary steps to address this trend.

While Bitcoin has existed since 2009, BTMs only recently became widely available. These kiosks, which allow individuals to buy or sell Bitcoins with deposited cash, were first introduced in 2013. While only approximately 1,200 BTMs were available in the United States at the end of 2017,[1] that number has since grown to over 32,000.[2] Today, BTMs are found in a variety of supermarkets, convenience stores, gas stations, restaurants, liquor stores, and laundromats.

As BTMs have become more prevalent and accessible, they increasingly have become a favored tool of criminals looking to prey upon elderly Americans. A 2021 FBI Public Service Announcement described the common features of this fraud. "The scammer often requests payment from the victim and may direct the victim to withdraw money from the victim's financial accounts, such as investment or retirement accounts. The scammers provide a QR code associated with the scammer's cryptocurrency wallet for the victim to use during the transaction. The scammer then directs the victim to a physical cryptocurrency ATM to insert their money, purchase cryptocurrency, and use the provided QR code to auto-populate the recipient address. Often the scammer is in constant online communication with the victim and provides step-by-step instructions until the payment is completed."[3]

---

[1] *See* Sari Harrar, *What to Know About Cryptocurrency ATMs and Why Criminals Love Them*, AARP, (Mar. 29, 2024), https://www.aarp.org/money/scams-fraud/info-2024/crypto-atm.html.

[2] *See Bitcoin ATMs in the United States*, COIN ATM RADAR, https://coinatmradar.com/country/226/bitcoin-atm-united-states/ (last visited Sept. 5, 2024).

[3] FEDERAL BUREAU OF INVESTIGATION, THE FBI WARNS OF FRAUDULENT SCHEMES LEVERAGING CRYPTOCURRENCY ATMS AND QR CODES TO FACILITATE PAYMENT (Nov. 4, 2021), available at https://www.ic3.gov/Media/Y2021/PSA211104.

This scheme has played out time and again in cities and towns across the United States. Earlier this summer, a small business owner in Springfield, Illinois, reported that a Coinhub BTM in his store repeatedly had been used by elderly individuals to deposit large sums of money at the urging of fraudsters. As he explained, "Scammers find these vulnerable people that aren't up on the latest technologies and they scare them on the phone, they tell them they are from the bank or the FBI and they are being watched, and they need to drop the money into this bitcoin machine."[4] Similar scenarios have played out in Texas,[5] California,[6] and seemingly every other state in the country.

According to data recently released by the Federal Trade Commission, BTM scams have exploded in recent years. Between 2020 and 2023, the amount consumers reported losing in this form of fraud increased nearly tenfold—from $12 million to $114 million. In the first half of this year alone, victims lost a whopping $65 million. And criminals are targeting elderly Americans, with people age 60 and older more than three times as likely to report a loss using a BTM than younger adults.[7]

Small business owners and everyday citizens have tried to step in and stop this increasing criminal activity on BTMs. The aforementioned small business owner in Springfield had the BTM removed from his store;[8] another Springfield shop owner taped a fraud warning to the screen of the BTM in his shop;[9] and a good Samaritan in Texas called 911 to enlist police assistance to stop an elderly woman in her 80s from depositing $40,000 of her savings in the Bitcoin wallet of a criminal.[10]

While the actions of these good Samaritans are laudable, they do not absolve Athena Bitcoin from taking all requisite steps to ensure your BTMs are not used to perpetuate fraud.

To better understand what actions Athena Bitcoin is taking to address this problem and what legislation may be necessary, we ask that you respond to the following questions no later than October 4, 2024:

1. Does Athena Bitcoin display a warning or other notification to customers that BTMs have been used to perpetuate fraud?

---

[4] David Blanchette, *No more bitcoin for one Springfield business*, ILLINOIS TIMES (July 26, 2024), available at https://www.illinoistimes.com/news-opinion/no-more-bitcoin-for-one-springfield-business-18836453#.

[5] Peyton Yager, *North Texas officer confronts man on phone scamming elderly woman: 'You freaking moron!'*, FOX4 NEWS (July 14, 2024), available at https://www.fox4news.com/news/white-settlement-scammer-phone-call-bitcoin-atm-scam-with-elderly-woman.

[6] *See, e.g.*, Queenie Wong, *Scammers exploit bitcoin ATMs. Will new California laws help crack down on fraud?*, Los Angeles Times (Oct. 22, 2023), available at https://www.latimes.com/california/story/2023-10-22/scammers-are-exploiting-bitcoin-atms-will-new-limits-help-crack-down-on-fraud.

[7] Emma Fletcher, *Bitcoin ATMs: A payment portal for scammers*, FEDERAL TRADE COMMISSION (Sept. 3, 2024), available at https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/09/bitcoin-atms-payment-portal-scammers.

[8] *See supra*, footnote 4.

[9] *See id.*

[10] *See supra*, footnote 5.

2. What form of identification, if any, does Athena Bitcoin require a customer to provide when making a deposit or other transaction? Does the form of identification differ depending on transaction size?
3. Does Athena Bitcoin have a minimum or maximum amount on the transaction size permitted on one of your BTMs?
4. Does Athena Bitcoin limit the amount an individual can deposit or transfer in a single day, week, or other period of time?
5. What is the average deposit and average transfer on an Athena Bitcoin BTM?
6. Does Athena Bitcoin hold deposited and transferred funds for any period of time or take any other measures to allow transactions to be reversed in the case of fraud or mistake? If not, does Athena Bitcoin warn customers that funds deposited in or transferred to another individual's Bitcoin wallet cannot be recovered even if the transaction was the result of fraud or mistake?
7. Does Athena Bitcoin insure depositors against fraud?
8. What customer support does Athena Bitcoin offer if an individual is defrauded?

We look forward to your prompt response.

Sincerely,

Richard J. Durbin
United States Senator

Richard Blumenthal
United States Senator

Elizabeth Warren
United States Senator

Tina Smith
United States Senator

Sheldon Whitehouse
United States Senator

Peter Welch
United States Senator

Jack Reed
United States Senator